Exhibit 11

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
Case No. 20-CV-954-WO-JLW

FARHAD AZIMA, Plaintiff, v. NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC., Defendants.	**DECLARATION OF MATTEO M. TOMASINI**

I, Matteo M. Tomasini, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am over 18 years of age and competent to make this declaration.

2. I make this declaration based on my personal knowledge, and if called as a witness, I could and would testify competently to the matters set forth in this declaration.

3. I am a Managing Director and the head of the cyber practice of Prescient Comply, LLC in New York, NY.

4. I was retained by Miller & Chevalier Chartered to opine on several matters relating to data belonging to Plaintiff Farhad Azima that was posted online and to provide expert witness testimony at trial.

5. Attached hereto as Exhibit A is a true and correct, authentic copy of the report (and attachments) I prepared and was provided to the Defendants on May 24, 2024. This report accurately represented my opinions at the time it was signed, and those opinions have not changed.

6. Attached hereto as Exhibit B is a true and correct, authentic copy of my supplemental expert report as attached to my initial report and provided to the Defendants on July 3, 2024. This supplemental expert report accurately represented my opinions at the time it was signed, and those opinions have not changed.

I declare under the penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on August 12, 2024 in New York, NY.

Matteo Tomasini

Matteo M. Tomasini

Exhibit A

May 24, 2024

EXPERT REPORT OF MATTEO TOMASINI

Farhad Azima v. Nicholas Del Rosso & Vital Management Services, Inc, United States District Court for the Middle District of North Carolina, 20-cv-954 (Internal Ref. No. 47776373)

I. QUALIFICATIONS

1. I am a Managing Director and head of the cyber practice of Prescient Comply, LLC ("Prescient"), where I have overseen all cyber operations since 2019. My curriculum vitae along with a list of my prior testimony for the past four years is provided in Appendix A.

2. I also co-founded a DDW data company called District 4 Labs for which, over the last 10 years, I personally collected thousands of databases containing tens of billions of compromised records. These datasets include hacked databases of companies and websites, malware dumps, and other databases with compromised PII. I also designed a database to store the data, and developed tools based on that data so DDW investigators can quickly and efficiently query those records for identifiers associated with individuals and companies. I continue to be involved in growing that business to include active engagement with the DDW to identify new sources and threat actors.

3. I am a recognized expert in the cyber security community: I have developed several open-source tools used by other practitioners; led internal corporate trainings on the Deep[1] and Dark Web[2] ("DDW") investigative tools and techniques; consulted on the development of third-party cyber tools and repositories; and contributed to discourse on various cyber community forums. I regularly attend cyber security conferences.

4. Prior to working at Prescient, I served as Director of Cyber Investigations & Threat Intelligence at BlueVoyant, a cybersecurity services company, from July 2017 to April 2019. At BlueVoyant, I managed DDW monitoring and investigations for the firm, conducted social media investigations, and was responsible for identifying, developing, and managing DDW-related

[1] The Deep Web is part of the internet that is not discoverable by means of standard search engines, including password-protected or dynamic pages and encrypted networks.
[2] The Dark Web is the part of the internet that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

metrics and risk factors to help assess third-party cyber risk.

5. From March 2013 until July 2017, I was employed at K2 Intelligence ("K2"), an investigative and risk analytics consulting firm, as an Analyst and moving up to Director of Cyber Defense. While at K2, I specialized in DDW investigations, social media intelligence, intellectual property theft, insider threats, due diligence, and Internet attribution, i.e., identifying individuals behind email addresses, usernames, and other online identifiers. I also served as the Technology Leader at K2 for two years during which time I led company-wide initiatives to identify and implement technologies used in traditional and cyber investigations.

6. My billing rate for this matter is $700 per hour. My compensation is in no way dependent on any outcome or opinions expressed in this case.

II. SCOPE OF ENGAGEMENT

7. I have been retained by Miller & Chevalier Chartered ("Miller" or the "Firm") to offer my expert opinion regarding data posted online that references Farhad Azima ("Azima").

8. Specifically, I was asked to identify and analyze online sites that host (1) links to files that at one point purportedly contained Azima's hacked data and/or (2) other content that appears to have been published as part of a campaign to smear Azima. I was also asked to preserve any identified content.

9. Additionally, I was asked to identify who was responsible for sending several suspected phishing emails to Azima and his associates in 2015 and 2016.

10. I reserve the right to amend, modify, or supplement this report if additional information or facts previously unknown to me are later brought to my attention.

III. SUMMARY OF CONCLUSIONS

11. It is my opinion based on common characteristics of the anti-Azima websites I identified that dozens of anti-Azima sources[3] were created by the same individual or group of individuals as part of a coordinated campaign targeting Azima. Among other indicators of a coordinated campaign, I found that these posts were created in three distinct time periods between 2016 and 2020 and contained similar language and images. I further note that several of these posts were made on social bookmarking sites and consisted of collections of links to the anti-Azima sources with similar language, images, and timing.

12. This anti-Azima campaign appears to have commenced at least as far back as 2016 when at least 15 such sources were online and continued until early 2020 when 44 anti-Azima sources were online. There were dramatic increases in anti-Azima sources in the years 2018 and 2019. The number of sources jumped from 15 to 25 in 2018 and from 29 to 44 in 2019. I identified at least 26 anti-Azima sources created on or after October 2017 containing links to Azima's personal data or language disparaging Azima or his businesses. The nature and characteristics of the anti-Azima sources we identified indicate that the individual or group behind this activity sought to share Azima's personal data with public audiences and publish negative content critical of Azima's business practices in a sustained and coordinated manner over several years.

13. It is also my opinion that at least seven of the 21 phishing emails received by Azima and his associates were likely sent by CyberRoot and/or BellTroX, Indian hacking companies. I believe this to be the case because these seven phishing emails contained links to domains that have been associated with CyberRoot and/or BellTroX.

[3] "Sources" is used throughout this report as a catch-all term to encompass websites, blogs, social media platforms, torrent sites, and other online sites with user-generated content.

IV. METHODOLOGY

A. Identification of Anti-Azima Sources

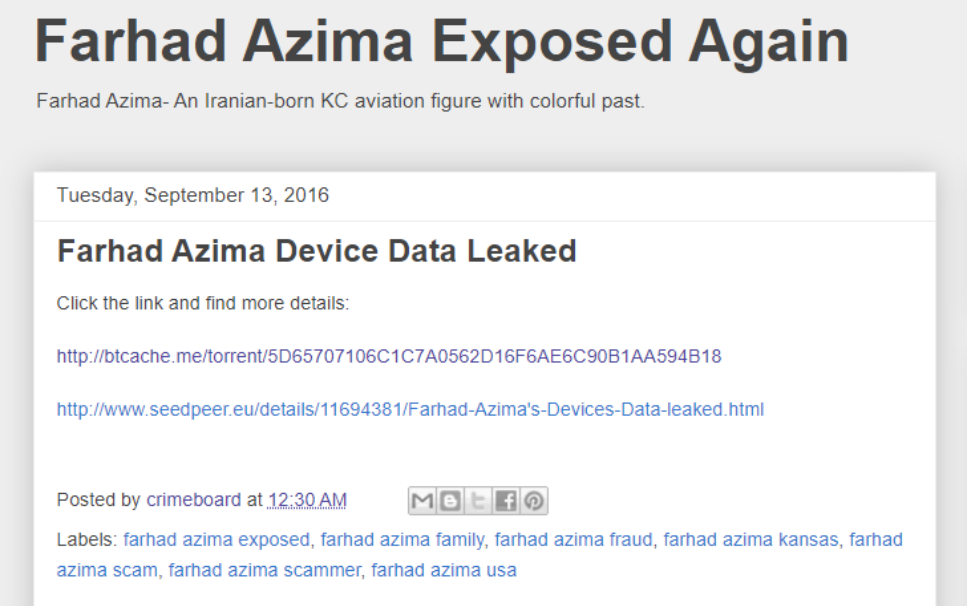
14. I was provided the URLs for two blog sites (farhadazimascams.blogspot[.]com and exposedfarhadazima.wordpress[.]com), and WeTransfer links associated with a WeTransfer account used to post what appears to have been data exfiltrated from Azima's devices. I was also provided with subpoena responses from Blogspot, WeTransfer, and WordPress containing information on the owners and primary contributors of the blog sites and the WeTransfer account. These subpoena responses included information about when the sites/accounts were created; names, email addresses, and usernames associated with the creators of these sites (if available); IP addresses associated with the site creators; and post upload/download/modification activity.

15. Following receipt of this information, I investigated the identifiers provided in the subpoena responses and reviewed content on the farhadazimascams[.]blogspot.com and exposedfarhadazima[.]wordpress.com sites. I identified nine publicly viewable posts issued between August and September 2016 on farhadazimascams[.]blogspot.com.

16. In addition to links to the WeTransfer file download and torrent sites[4] (some of which are now defunct), I found dozens of comments to the posts on these sites made between 2016 and 2019. These comments were generally made by anonymous users and often contained links to other websites with user-generated content. An example of a September 13, 2016 post on farhadazimascams[.]blogspot.com with these accompanying comments is shown below.[5]

[4] Torrent sites host torrents, a communication protocol for peer-to-peer file sharing, which enables users to distribute data and electronic files over the Internet in a decentralized manner.

[5] **See:** https://farhadazimascams.blogspot[.]com/2016/09/farhad-azima-device-data-leaked.html



Farhad Azima Exposed Again

Farhad Azima- An Iranian-born KC aviation figure with colorful past.

Tuesday, September 13, 2016

Farhad Azima Device Data Leaked

Click the link and find more details:

http://btcache.me/torrent/5D65707106C1C7A0562D16F6AE6C90B1AA594B18

http://www.seedpeer.eu/details/11694381/Farhad-Azima's-Devices-Data-leaked.html

Posted by crimeboard at 12:30 AM

Labels: farhad azima exposed, farhad azima family, farhad azima fraud, farhad azima kansas, farhad azima scam, farhad azima scammer, farhad azima usa

4 comments:

Anonymous September 26, 2016 at 2:55 AM

who is this idiot?

Reply

Anonymous July 17, 2018 at 10:55 PM

it was a real scam done by farhad azima
http://www.sociopost.com/taxonomy/term/991389

Reply

Anonymous August 1, 2018 at 4:21 AM

Authorities are investigating Farhad Azima as part of a global corruption case.

https://exposedfarhadazima.wordpress.com/2016/09/05/shocking-truth-about-farhad-azima/

https://flipboard.com/@farhadazima2018/farhad-azima-d366uthty

https://remote.com/farhadazima

Reply

Anonymous January 10, 2019 at 4:05 AM

new update about farhad azima
https://www.booksie.com/578656-the-ugly-truth-about-farhad-azima-scam.-read-or-miss-out

Reply

17. After finding these comments on the Blogspot and Wordpress sites, I visited and investigated the sites linked in those comments. In many cases, that investigation led to the

discovery of additional sites and posts, which I then used to discover additional sites and posts. For example, I identified a May 25, 2018 comment posted by an anonymous user to a September 20, 2016 post on farhadazimascams[.]blogspot.com that contained a link to a post on the website Wattpad.[6]

5 comments:

Anonymous September 22, 2016 at 4:17 AM

such a fucking scammer

Reply

Anonymous May 25, 2018 at 2:56 AM

latest links of farhad azima
https://www.wattpad.com/309140201-latest-links-of-farhad-azima%27s-scam-new-links-of

Reply

sturat June 12, 2018 at 12:36 AM

seriously this scam shamed US
https://farhadazima.wordpress.com/

Reply

Anonymous July 17, 2018 at 10:44 PM

https://commons.wikimedia.org/wiki/File:Farhad_Azima_Breaking_News.jpg

Reply

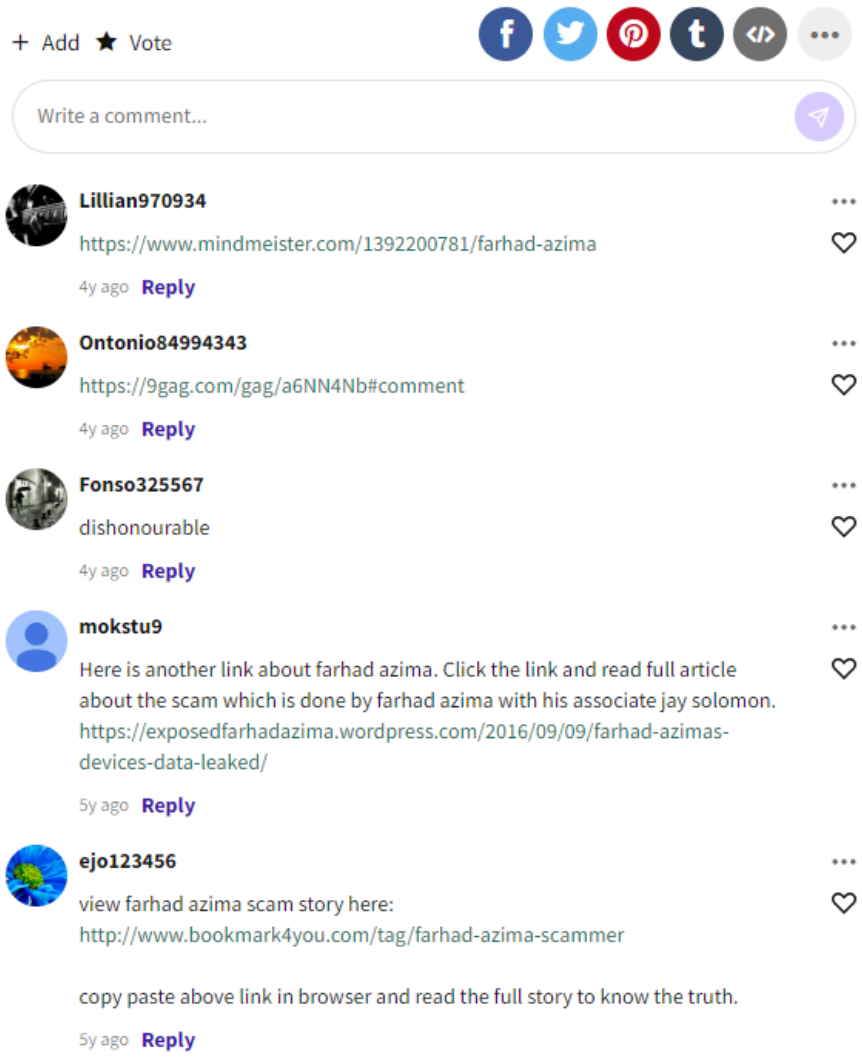
Anonymous January 10, 2019 at 4:02 AM

find more information @
https://www.reddit.com/user/jenny9864/comments/8w9ih3/farhadazimafraud/

Reply

18. I investigated the Wattpad link and found that it contained several comments by other Wattpad users which in turn included links to other anti-Azima content on the websites Mindmeister and 9gag.[7]

[6] **See:** https://farhadazimascams.blogspot[.]com/2016/09/scams-that-shamed-us.html
[7] **See:** https://www.wattpad.com/309140201-latest-links-of-farhad-azima%27s-scam-new-links-of



19. I was able to repeat a similar process in my investigation of exposedfarhadazima.wordpress[.]com and several other connected sites and platforms to discover an expansive universe of anti-Azima sources.

20. During this process, I identified dozens of accounts, aliases, names, distinct language, and other identifying information associated with these anti-Azima sources. I conducted searches for these identifiers on the surface, Deep, and Dark Web, as well as a proprietary database of over 45 billion breached credentials.[8] In some cases, this led to the discovery of additional anti-

[8] The surface web is the part of the internet indexed and made searchable by various search engines.

Azima websites.

21. I was also provided subpoena responses from numerous platforms I found hosting this content, including identifiers that were analyzed by using the above-mentioned methods in order to attempt to discover more anti-Azima sources.

B. Anti-Azima Website Preservation

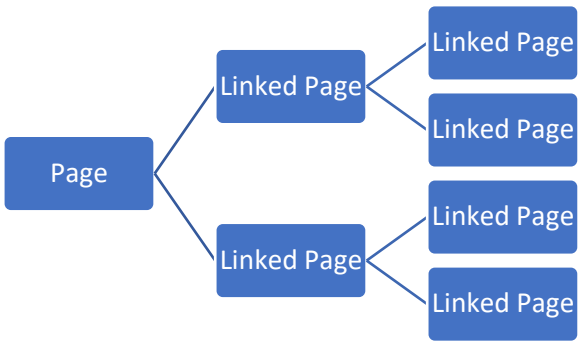
22. During my analysis, I directed the capture and preservation of the anti-Azima sources using the following methods.

23. The pages were captured using Page Vault software, which documents the details of the capture (such as date and time; browser information; and capturing user, or "collector") and attaches a unique hash value to each capture for later authentication purposes.[9] Page Vault uses a remote browser, which prevents the collector from modifying any content on the page or its source code.[10]

24. For pages which required a user login to view, I used an examiner account (sometimes known as a "sockpuppet"). I did not interact with any other users of the sites, or request connection (or "friend") with any accounts.

25. I was initially provided with the URLs for two websites to capture: farhadazimascams[.]blogspot.com and exposedfarhadazima[.]wordpress.com. As part of my analysis, I discovered several other websites I believe were connected to the case and preserved them as well. For each URL, I captured the page with Page Vault, and reviewed its contents for links to additional pages. I then captured those linked pages and repeated the process of review and capture until all related pages were identified and captured.

[9] **See:** https://blog.page-vault.com/why-its-important-to-preserve-the-chain-of-custody-for-digital-evidence
[10] **See:** "How Legal Teams Use Self-Directed Software to Collect Admissible Online Evidence," Page Vault white paper published October 2023, https://blog.page-vault.com/how-legal-teams-use-self-directed-software-to-collect-admissible-online-evidence



26. I documented these pages in a spreadsheet, which tracked the URL, unique Page Vault Capture ID, and linked URLs for each, so the source of the captured URL could be identified in later analysis. I additionally documented the original and ultimate URLs for any redirected pages, and whether the page was currently online or defunct.

27. Because of incompatibility between Page Vault's browser and certain sites, I captured two of the 391 sites using a different software, Hunchly.[11] Hunchly is a software that Prescient uses in conjunction with a local web browser to capture pages as they are loaded passively, rather than at the specific direction of the collector.[12]

C. Investigation of Phishing Emails

28. I received 21 suspected phishing emails received by Azima and his associates between 2005 and 2016.

29. I was also provided with a December 2022 report authored by Meta titled "Threat Report on the Surveillance-for-Hire Industry" ("Meta Report"), which, among other details, includes an analysis of CyberRoot, which the Meta Report alleges is a surveillance-for-hire firm, i.e., a hacking firm.[13] The Meta Report concludes that CyberRoot uses tactics similar to those of another Indian surveillance-for-hire firm named BellTroX and that, according to public reporting,

[11] These were https://www.plurk[.]com/FarhadAzima and https://www.reddit[.]com/r/memes/comments/cz4gw0/farhad_azima_and_khater_massaad_latest_news/
[12] **See:** https://support.hunch.ly/category/50-hunchly-evidence-guide
[13] **See:** https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

CyberRoot and BellTroX have a history of working together and have shared the same web infrastructure and employees.[14] [15] The report also includes a list of indicators of compromise—phishing links and domains—associated with CyberRoot that were used to conduct their phishing campaigns. I investigated whether the phishing emails received by Azima and his associates contained the same tactics and infrastructure used by CyberRoot as detailed in the Meta Report.

30. Following receipt of this information, I analyzed the forensic data[16] contained in the suspected phishing emails received by Azima and his associates. I identified at least 15 links contained in the emails that indicate they were designed to conduct phishing attacks. The formats of the email messages and corresponding references to social media domains outside of the domain portion of the link, (e.g. "youtube.com" featured in link of xxxx.com/youtube.com), suggest to me that the links redirected to websites made to look like the login pages for various social media and other online platforms. Such sites are often designed to steal victims' login credentials and/or can also be used to infect their devices with malware.

31. For example, a May 19, 2015 email sent to Azima's email address "fa@fa1.us" was designed to look like a LinkedIn notification indicating Azima had received a message from another user. In that email message, I identified a link (in the "View Message" button, shown in the screenshot of the email, below) that contained the following URL:

> http://www.2ntigv4chn2hbk.mesvr[.]com/tg/2ntigv4chn2hblhttp/accounts-linkedin-com-servicelogin-addsession-v-en-us.look-com.org/-continue-https-maiil.gooogle.com-maiil.u.1.serviice-maiil.rpsnv.11-ct-1347523076345434376 4-rver.post/?to=&adroid=//accounts-linkedin-com-servicelogin-addsession-v-en-us.look-com.org/-continue-https-maiil.gooogle.com-maiil.u.1.serviice-maiil.rpsnv.11-ct-1347523076345434376 4-rver.post/m/?to=&msg=&red=//linkedin[.]com

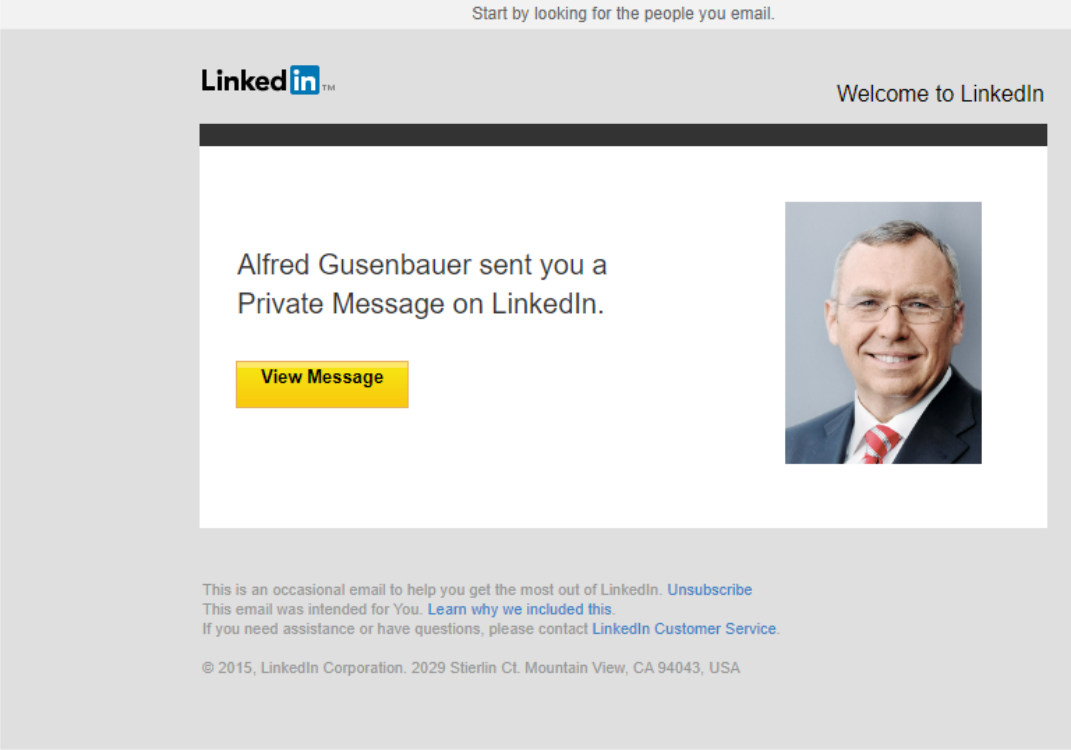
[14] **See:** https://www.reuters.com/article/cyber-lawsuit-belltrox/lawsuit-accuses-indian-hackers-of-leaking-businessmans-emails-idUSKBN2742EN/

[15] **See:** https://www.bloomberg.com/news/articles/2020-10-19/u-s-businessman-says-hacker-for-hire-firms-stole-his-data

[16] Forensic data is defined here and used in this report to refer to forensic objects that may or may not have some forensic value to an investigation. Among other elements, forensic data can include IP addresses, URLs, timestamps, logs, and files.

32. The link redirects victims to the domain look-com[.]org (highlighted in the above URL), among other domains. I note that the initial domain of "mesvr[.]com" is an online service designed to let users know when an email has been read.

From: "<Linkedin>" <messages-N0reply-linkedin@tech-center.com>
Sent: 5/19/2015 12:39:47 PM +0200
To: fa@fa1.us
Subject: Alfred Gusenbauer sent you a Private Message on LinkedIn.



33. I investigated look-com[.]org and the other domains contained in the links in the phishing emails. That investigation led me to discover various identifiers and other information relating to the domains including, but not limited to, domain registration records and associated IP addresses.

34. During this process, I identified dozens of IP addresses, domain registration records, and other identifying information associated with the domains. I then used those identifiers to further investigate the network infrastructure and any identifiable individuals or

organizations associated with the domains. I conducted searches on the surface, Deep, and Dark Web, a proprietary database of over 45 billion breached credentials, as well as open source and commercial investigative tools for investigating domains and associated network infrastructure.

35. My investigation of the identifiers associated with the phishing emails led me to locate a report and data published by the Citizen Lab[17] titled "Dark Basin: Uncovering a Massive Hack-For-Hire Operation" that focuses on Dark Basin, a hack-for-hire group that the Citizen Lab links to BellTroX with "high confidence."[18] The report includes a link to a folder on developer platform GitHub that contains a list of indicators of compromise ("IOCs") associated with Dark Basin including, among other indicators, domains and domain registrant email addresses tied to the group's hacking activities and network infrastructure they use(d). I utilized this data to investigate potential connections between the phishing emails and Dark Basin, BellTroX, and CyberRoot.

V. ANALYSIS: ANTI-AZIMA SOURCES

A. At Least 84 Sites/Pages Containing Links to Azima's Hacked Data or Anti-Azima Posts were Created from 2016 to Present, of which 26 were Created from October 2017 to Present

36. I identified a large number of anti-Azima sources that have been created since 2016. To date, I have identified 84 websites, blogs, social media platforms,[19] and other content-forward platforms that hosted anti-Azima information. Those 84 sites are:

- 1337x.to
- about.me
- adfty.biz
- angelfire.com
- artwanted.com
- bagtheweb.com

[17] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada, that conducts research on information and communication technologies, human rights, and global security. It is considered a credible source when it comes to spyware research.
[18] **See:** https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf
[19] In some cases, Prescient identified several social media accounts on a given social media platform hosting anti-Azima information.

- bebee.com
- behance.net
- bepress.com
- bibsonomy.org
- blogspot.com
- bookmark4you.com
- booksie.com
- bravesites.com
- briefingwire.com
- btcache.me
- commaful.com
- diigo.com
- discussion.community
- dribbble.com
- e27.co
- flipboard.com
- folkd.com
- freeprnow.com
- goodreads.com
- gravatar.com
- gust.com
- headshotcrew.com
- hubski.com
- imgflip.com
- imgur.com
- innovatorsedge.io
- livejournal.com
- medium.com
- memonic.com
- mendeley.com
- metatorrents.net
- mindmeister.com
- monova.org
- myfolio.com
- mystrikingly.com
- over-blog.com
- own-free-website.com
- pastebin.com
- pearltrees.com
- pinterest.com
- plurk.com
- poemhunter.com
- posteezy.com
- proboards.com
- professionalontheweb.com
- reddit.com
- remote.com
- schoolofeverything.com
- scoophot.com
- seedpeer.eu
- seekingalpha.com
- skyrock.com
- slashdot.org
- snapzu.com
- sociopost.com
- soup.io
- sparkpeople.com
- speakerdeck.com
- stage32.com
- steepster.com
- storybird.com
- sumotorrent.sx
- symbaloo.com
- the-dots.com
- thepiratebay.org
- triberr.com
- ttlink.com
- uniquethis.com
- voat.co
- wattpad.com
- wellfound.com
- wetransfer.com
- wordpress.com (5)
- zumvu.com

37. I identified data on 44 of these anti-Azima sources which indicate the sites were created or began hosting anti-Azima content between August 2016 and January 2020, broken down as follows:

- 2016 – 16 anti-Azima sources[20]
- 2017 – One anti-Azima source
- 2018 – 11 anti-Azima sources
- 2019 – 13 anti-Azima sources
- 2020 – Two anti-Azima sources

38. I was able to determine that 26 of these anti-Azima sources were created or began hosting anti-Azima information after October 2017 and that, as described below, these sources appear to be part of a coordinated campaign targeting Azima.

39. The abovementioned anti-Azima sources can be divided into the following categories.[21]

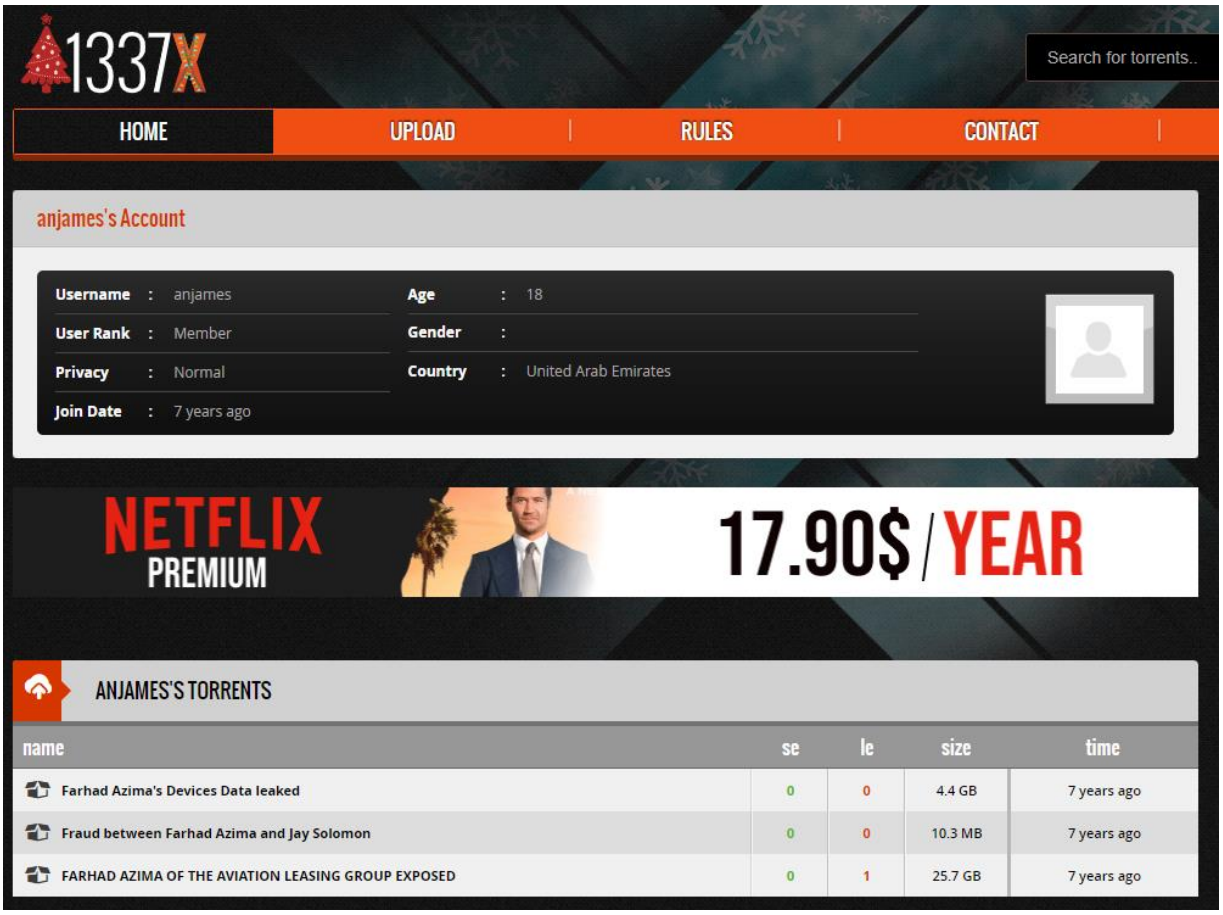
40. **Torrent Sites:** Prescient identified seven torrent sites. As of January 2024, two of these torrent sites contain links to torrent files which appears to contain metadata that would have allowed a user to download Azima's data (it was not possible to download the data because the torrents did not have any active seeders,[22] but the meta-data of the torrent files indicate they contain Azima's data). Five of the torrent sites are currently offline, but based on their titles and/or context, appear to have at some point provided users with the ability to download at least some of Azima's data. The seven torrent sites are:

- thepiratebay[.]org/torrent/15484452 - **active**
- 1337x[.]to/user/anjames/ - **active**[23]
- btcache[.]me/torrent/5d65707106c1c7a0562d16f6ae6c90b1aa594b18 - **defunct**

[20] On some of the identified anti-Azima sources, activity (such as additional posts, updates, or other forms of activity) was detected after this date. This year of demarcation is specifically the date that the anti-Azima source was created or first logged activity, but does not necessarily indicate that further activity was not detected in subsequent years.
[21] Categories are not mutually exclusive, as some sites identified cover multiple categories.
[22] Seeders are torrent site users who are sharing a file(s) with other users.
[23] This webpage for the user "anjames" provides links to three torrents.

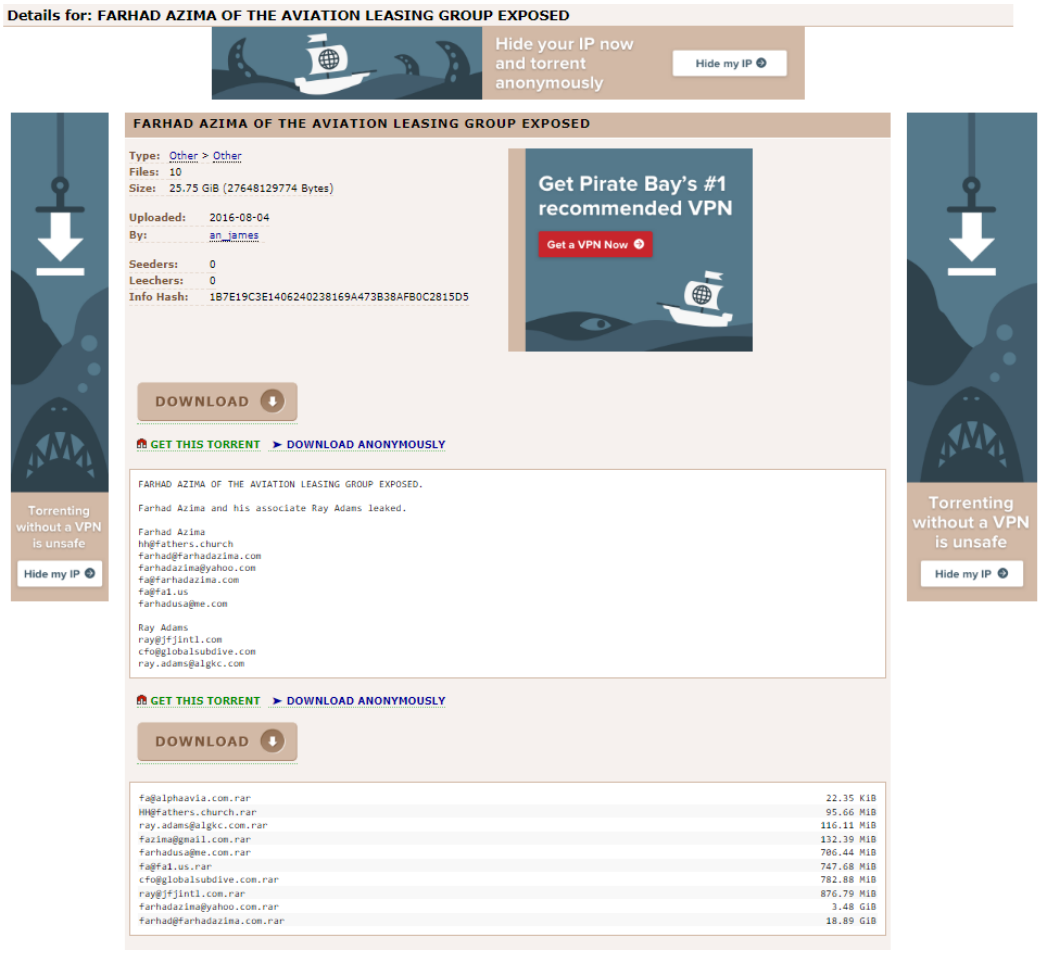
- metatorrents[.]net/torrent/15484452/farhad+azima+of+the+aviation+leasing+group+exposed - **defunct**
- sumotorrent[.]sx/en/details_10762203.html - **defunct**
- seedpeer[.]eu/details/11694381/farhad-azima's-devices-data-leaked.html - **defunct**
- monova[.]org/42248895 - **defunct**

41. Prescient identified file upload date information on the two active torrent sites. Approximately seven years ago, an account under the username "anjames" with a reported location of United Arab Emirates and a listed age of 18 uploaded three torrent files containing what appears to be Azima's data to torrent website 1337x.[24]



[24] **See:** https://1337x[.]to/user/anjames/

42. In addition, on August 4, 2016 an account under the username "an_james" uploaded a torrent file containing what appears to be Azima's data to torrent website thepiratebay.org.[25]



43. **Websites Containing Links to Azima's Data on WeTransfer:** I identified three websites that host links to files on file sharing website WeTransfer that at one point purportedly contained data taken from devices maintained by Azima. Those three websites are: farhadazimascandal.page[.]tl, exposedfarhadazima.wordpress[.]com, farhadazimascams.blogspot[.]com.

44. On an unknown date, an anonymous user posted links to file sharing website

[25] **See:** https://thepiratebay[.]org/torrent/15484452

WeTransfer (hyperlinked via "Download" text prompt in screenshot, below) on website farhadazimascandal.page[.]tl.[26] The webpage also included a link that directed users to the torrent files on thepiratebay[.]org described above.

farhad azima

FARHAD AZIMA

Farhad Azima is such a big scammer. Some reports claim that he found guilty in US major scams though Azima has always claimed that he know nothing.

Find some links to read more about Farhad Azima scandal:

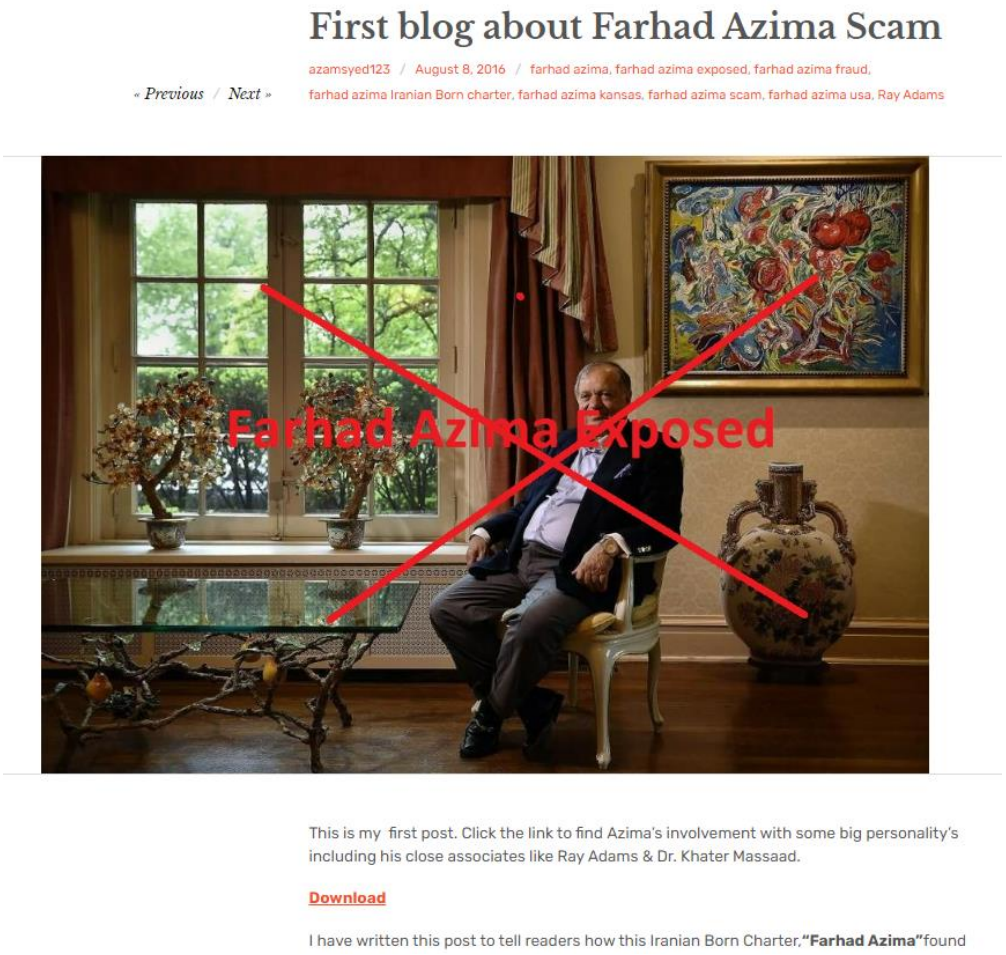
https://thepiratebay.org/torrent/15484452

Download

45. On an unknown date between August 8, 2016 and June 9, 2019 an account under the username "azamsyed123" posted a link to the file sharing website WeTransfer on exposedfarhadazima.wordpress[.]com.[27] These links were hyperlinked in a "Download" text prompt as show in the screenshot below. During approximately the same time period, the creator of the website also posted links to files that purportedly contained Azima's data hosted on various torrent websites.

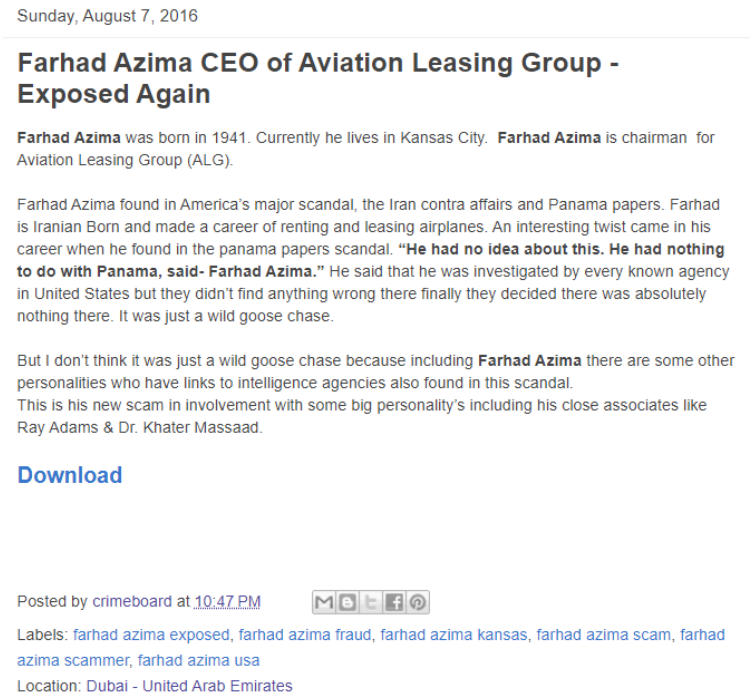
[26] **See:** http://farhadazimascandal[.]page.tl/

[27] **See:** https://exposedfarhadazima.wordpress[.]com/2016/08/08/farhad-azima-farhad-azima-scammer/



46. On an unknown date between August 7, 2016 and June 6, 2019 an account under the username "crimeboard" posted a link to the file sharing website WeTransfer on blog site farhadazimascams.blogspot[.]com.[28] This link was hyperlinked in a "Download" text prompt as show in the screenshot below. The post containing the link says that the post was made from Dubai, United Arab Emirates, with the GPS coordinates 25°12'17.5"N 55°16'14.8"E.[29] During approximately the same time period, the creator of the website also posted links to files that purportedly contained Azima's data hosted on various torrent websites.

[28] **See:** https://farhadazimascams.blogspot[.]com/2016/08/farhad-azima-ceo-of-aviation-leasing.html
[29] Which geolocate to the general location of Al Safa Street, Dubai, United Arab Emirates.



Sunday, August 7, 2016

Farhad Azima CEO of Aviation Leasing Group - Exposed Again

Farhad Azima was born in 1941. Currently he lives in Kansas City. **Farhad Azima** is chairman for Aviation Leasing Group (ALG).

Farhad Azima found in America's major scandal, the Iran contra affairs and Panama papers. Farhad is Iranian Born and made a career of renting and leasing airplanes. An interesting twist came in his career when he found in the panama papers scandal. **"He had no idea about this. He had nothing to do with Panama, said- Farhad Azima."** He said that he was investigated by every known agency in United States but they didn't find anything wrong there finally they decided there was absolutely nothing there. It was just a wild goose chase.

But I don't think it was just a wild goose chase because including **Farhad Azima** there are some other personalities who have links to intelligence agencies also found in this scandal.
This is his new scam in involvement with some big personality's including his close associates like Ray Adams & Dr. Khater Massaad.

Download

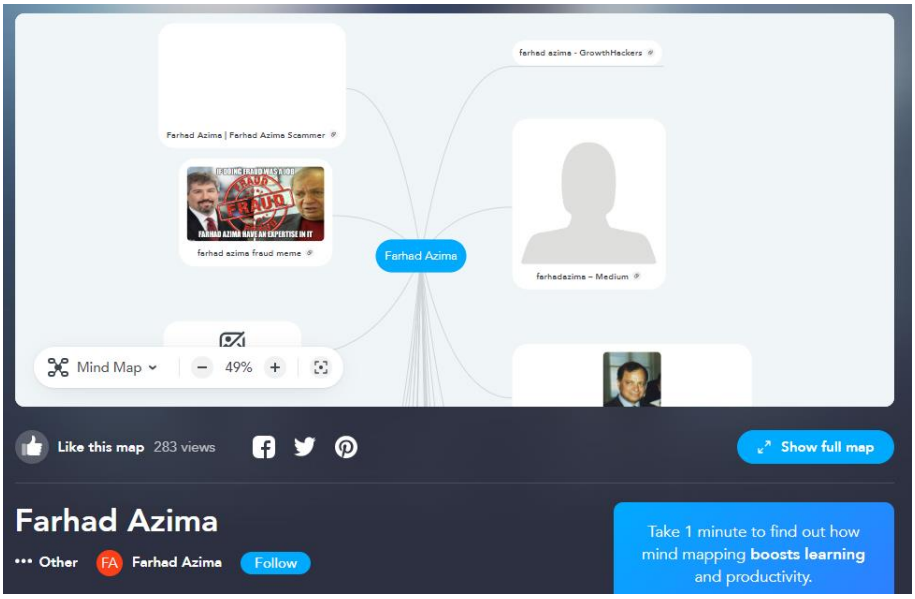
Posted by crimeboard at 10:47 PM

Labels: farhad azima exposed, farhad azima fraud, farhad azima kansas, farhad azima scam, farhad azima scammer, farhad azima usa
Location: Dubai - United Arab Emirates

47. **Websites and Social Media Platforms that Include Links to Websites with Links to Torrents or WeTransfer:** I identified at least 38 websites and social media platforms that include links to the abovementioned sites that contained links to torrent sites or WeTransfer as described above. These anti-Azima sources were created or contain posts that were published between August 2016 and January 2020.

48. The most recent site that I found was on the mind mapping social media platform MindMeister. [30] According to data obtained from the platform via a subpoena request, on an unknown date between January 2, 2020 and January 16, 2020 an account under the name "Farhad Azima" created a mind map with links to exposedfarhadazima.wordpress[.]com and other sites with anti-Azima information.

[30] **See:** https://www.mindmeister[.]com/1392200781/farhad-azima



49. **Websites and Social Media Accounts Critical of Azima's Business Practices:** In addition to the abovementioned anti-Azima sources, I identified several other websites and social media accounts that contain content critical of Azima's business practices. These anti-Azima sources were created or published posts between August 2016 and January 2020. Most of these anti-Azima sources include content accusing Azima of being part of a fraudulent scheme. For example, a December 16, 2019 post titled "SOME BIGGEST FRAUDS AND THEIR DOER" was published by an unknown actor on blog farhadazima.over-blog[.]com, a blog site created with a URL that includes Azima's name.[31] Among other accusations, the blog post accuses Azima and several other individuals of being "scammers" and "conmen."

[31] **See:** http://farhadazima.over-blog[.]com/2019/12/some-biggest-frauds-and-their-doer.html

JHO LOW, RANDY GLASS, WILL Z. MCFARLAND, YVONNE BANNIGAN, FARHAD AZIMA, KHATER MASSAAD, A HOLLYWOOD EXECUTIVE IMPERSONATOR

SOME BIGGEST FRAUDS AND THEIR DOER

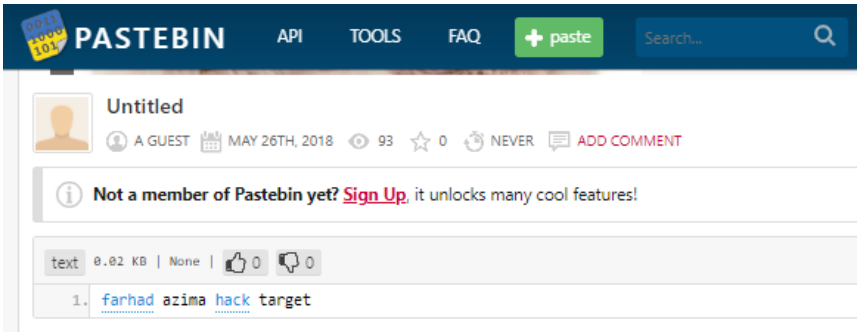
DECEMBER 16 2019

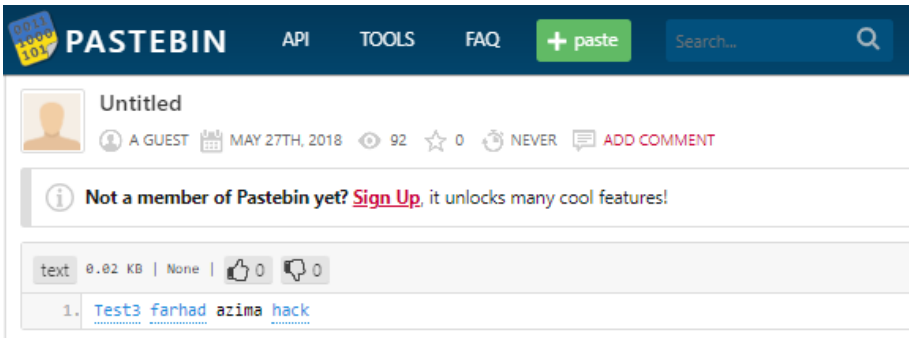
In this article, I am going to highlight some biggest fraud which I have read till now. And would like to share with people how they can take get experience from these real-life fraudsters. I am sure it provides some insight to people who are already on hard time and can face some near situation in their near future because scammers take advantage of those innocent people. The inside reality is, there are always people (scammer/fraudster) out there who looking for people (victims) they can easily get advantage of them. You can also find number of scammers/conmen on cyber space. Farhad Azima, Jay Solomon, Dr. Khater Massaad, Ray Adams, Jho Low, Randy Glass, Will Z. McFarland, Yvonne Bannigan, A Hollywood executive impersonator are few of them.

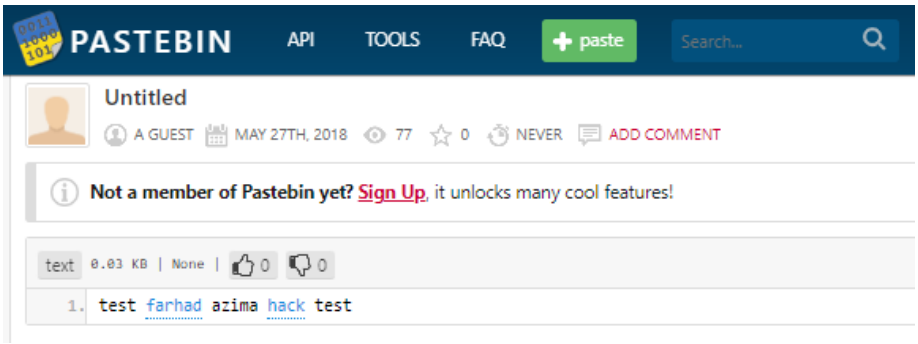
50. **Paste Sites with References to Azima and Hacking:** I identified eight posts on paste site Pastebin published between May 26, 2018 and June 1, 2018 that reference Azima and hacking, with several appearing to refer to him as a "target."[32] [33] [34] [35] [36] [37] [38] [39] Paste sites are sites that allow users to store and share text-based information. Paste sites typically provide users with a simple interface to paste their content, which is then saved as a unique URL that can be shared with others. Paste sites are often used by cybercriminals to share information anonymously. Owing

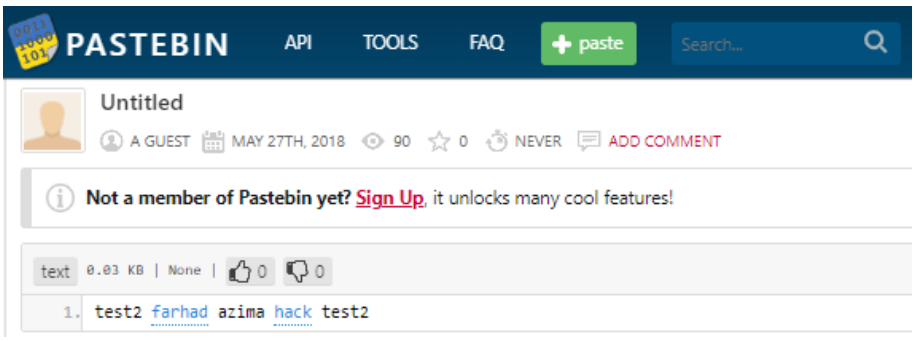
[32] **See:** https://pastebin[.]com/EZ8MpsZG
[33] **See:** https://pastebin[.]com/YkEFCnv0
[34] **See:** https://pastebin[.]com/34q1W1mn
[35] **See:** https://pastebin[.]com/f0S6Nd61
[36] **See:** https://pastebin[.]com/ns7buKZY
[37] **See:** https://pastebin[.]com/Ne8MK66e
[38] **See:** https://pastebin[.]com/e7fnzK2r
[39] **See:** https://pastebin[.]com/pPxy3N58

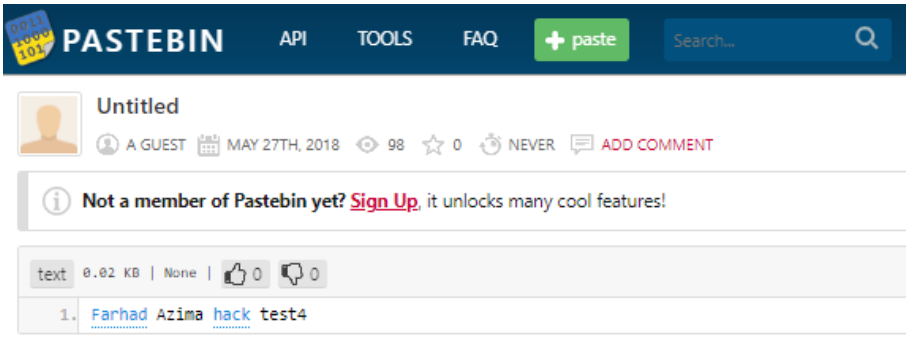
to a lack of contextual information relating to these posts, I was unable to determine their purpose or intent. Screenshots of these sites are included below:

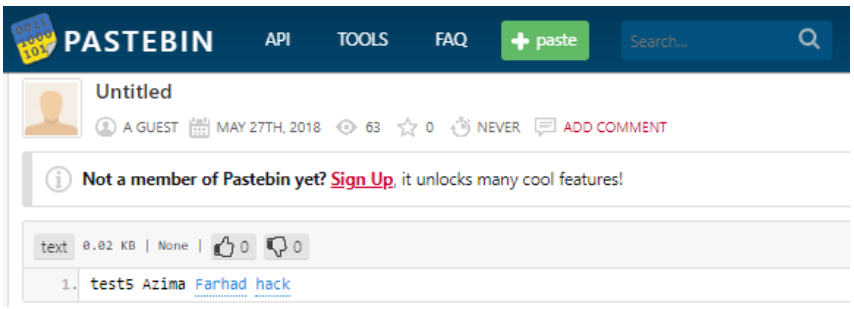


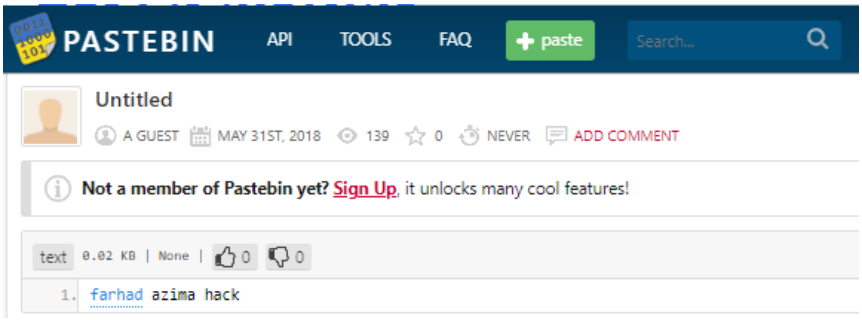


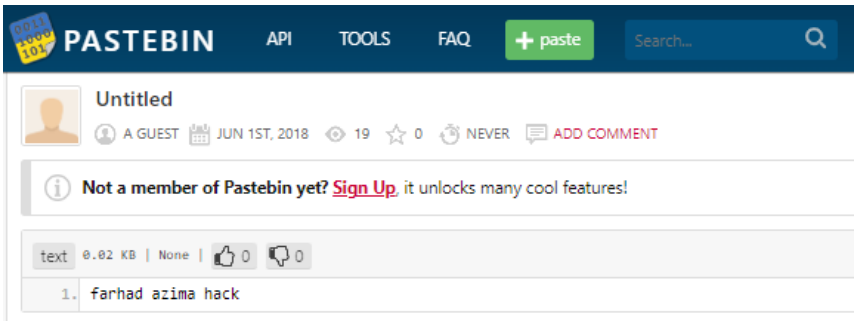










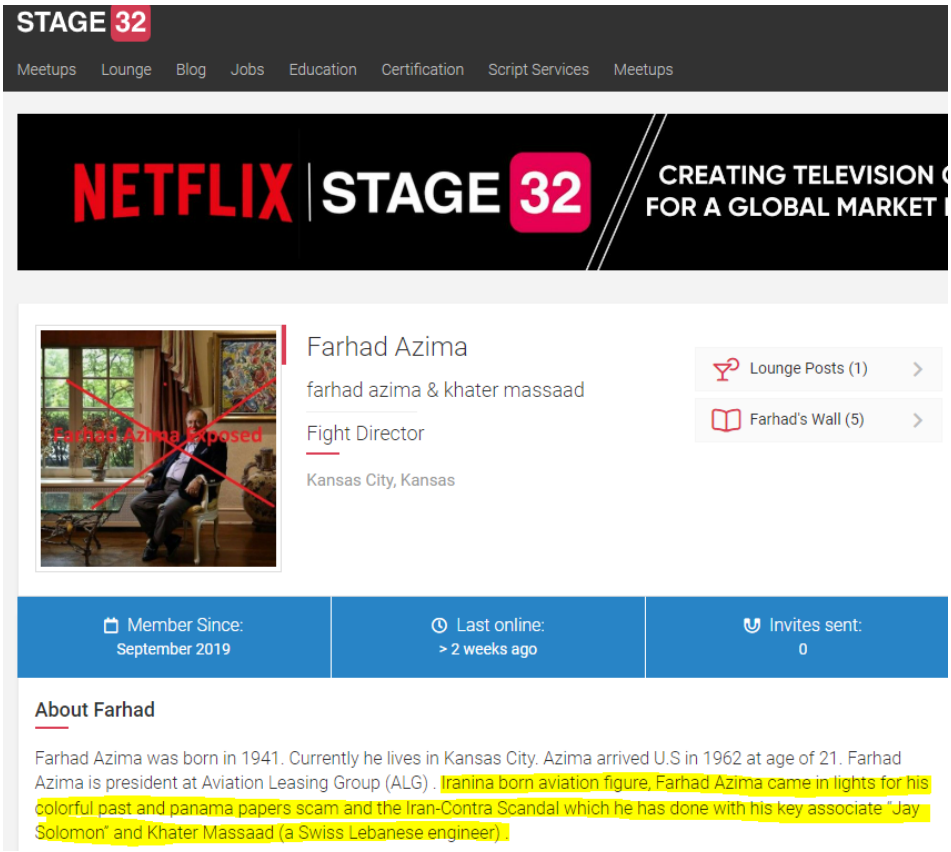


B. The Anti-Azima Sites Share Common Indicators Suggesting They Are Part of a Coordinated Campaign

51. It is my opinion that the abovementioned anti-Azima sources appear to be connected and are part of a coordinated campaign targeting Azima perpetrated by the same person

or group of people. My reasoning for this opinion is detailed below.

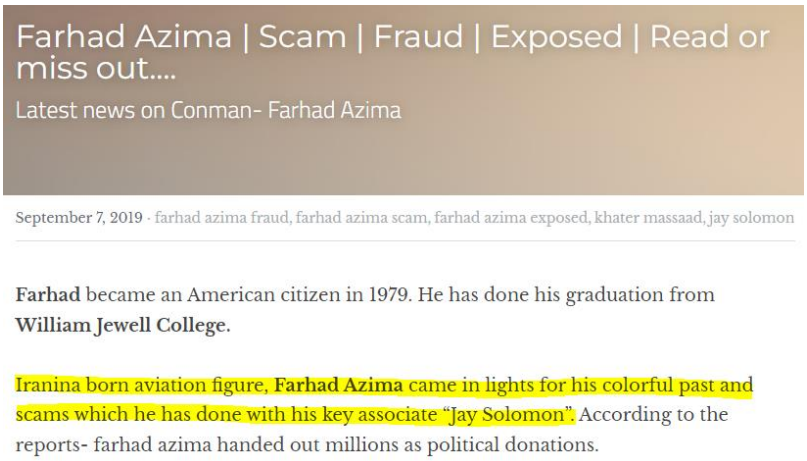
52. **Similar Language Use and Style of Writing:** Many of the anti-Azima sites that I found feature similar, if not the exact same language and style of writing, including the exact same typo. For example, I identified an account created in September 2019 under the name "Farhad Azima" on social media platform Stage 32 that has an "About" section that includes the following sentence, "Iranina [sic] born aviation figure, Farhad Azima came in lights for his colorful past and panama papers scam and the Iran-Contra Scandal which he has done with his key associate 'Jay Solomon' and Khater Massaad (a Swiss Lebanese engineer) ."[40]



53. The near exact same language was identified in a September 7, 2019 post identified on blog site farhadazimasite.mystrikingly[.]com that includes the wording, "Iranina [sic] born

[40] **See:** https://www.stage32[.]com/farhadazima

aviation figure, Farhad Azima came in lights for his colorful past and scams which he has done with his key associate 'Jay Solomon'."[41]


Farhad Azima | Scam | Fraud | Exposed | Read or miss out....

Latest news on Conman- Farhad Azima

September 7, 2019 · farhad azima fraud, farhad azima scam, farhad azima exposed, khater massaad, jay solomon

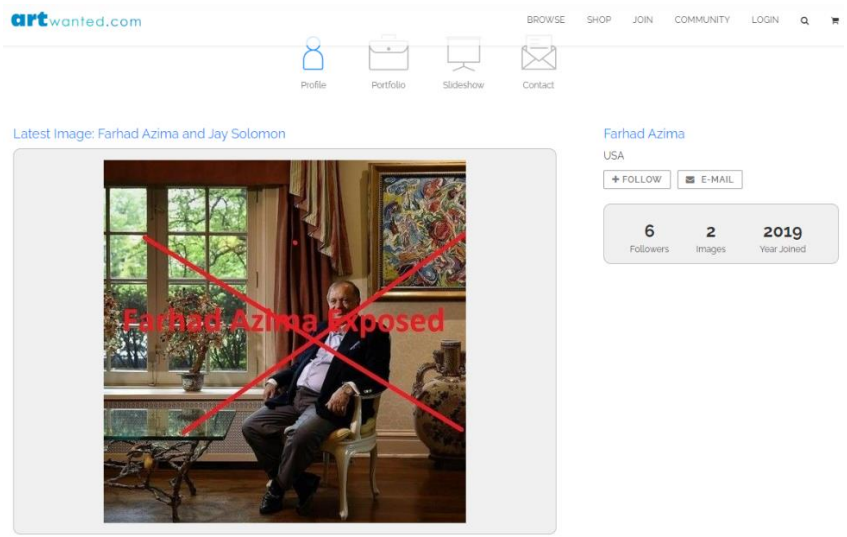
Farhad became an American citizen in 1979. He has done his graduation from **William Jewell College.**

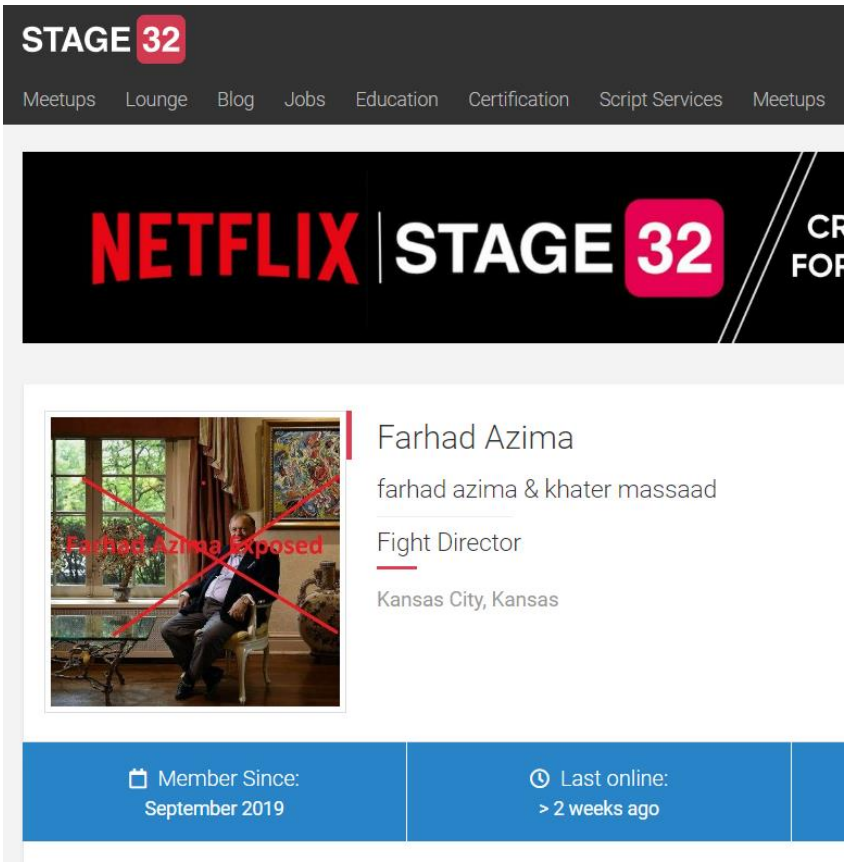
Iranina born aviation figure, **Farhad Azima** came in lights for his colorful past and scams which he has done with his key associate "Jay Solomon". According to the reports- farhad azima handed out millions as political donations.

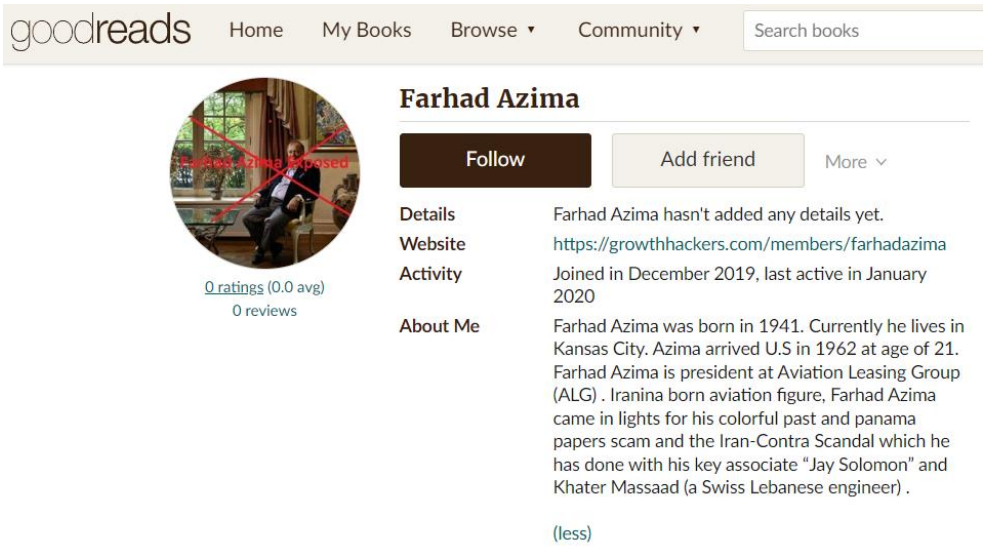
54. Both sites include the identical misspelling of Iranian ("Iranina") and usage of quotation marks around the name "Jay Solomon." Both also use the distinctive phrase "came in lights for his colorful past." I am of the opinion that it is very unlikely that these similarities of language use and writing are random, and it is more likely that these posts were created by the same individual(s) as part of a coordinated effort to smear Azima.

55. **Duplication of Images:** Dozens of the anti-Azima sites that I found include the same images featuring Azima. In particular, I observed the repeated use of an image of Azima with red lines in the shape of an "X" and red text that read "Farhad Azima Exposed." A representative sample of anti-Azima sources that include the duplicative use of such images is shown below.[42] [43] [44]

[41] **See:** https://farhadazimasite.mystrikingly[.]com/blog/farhad-azima-scam-fraud-exposed-read-or-miss-out
[42] **See:** https://www.artwanted[.]com/farhadazima
[43] **See:** https://www.stage32[.]com/farhadazima
[44] **See:** https://www.goodreads[.]com/user/show/106321378-farhad-azima

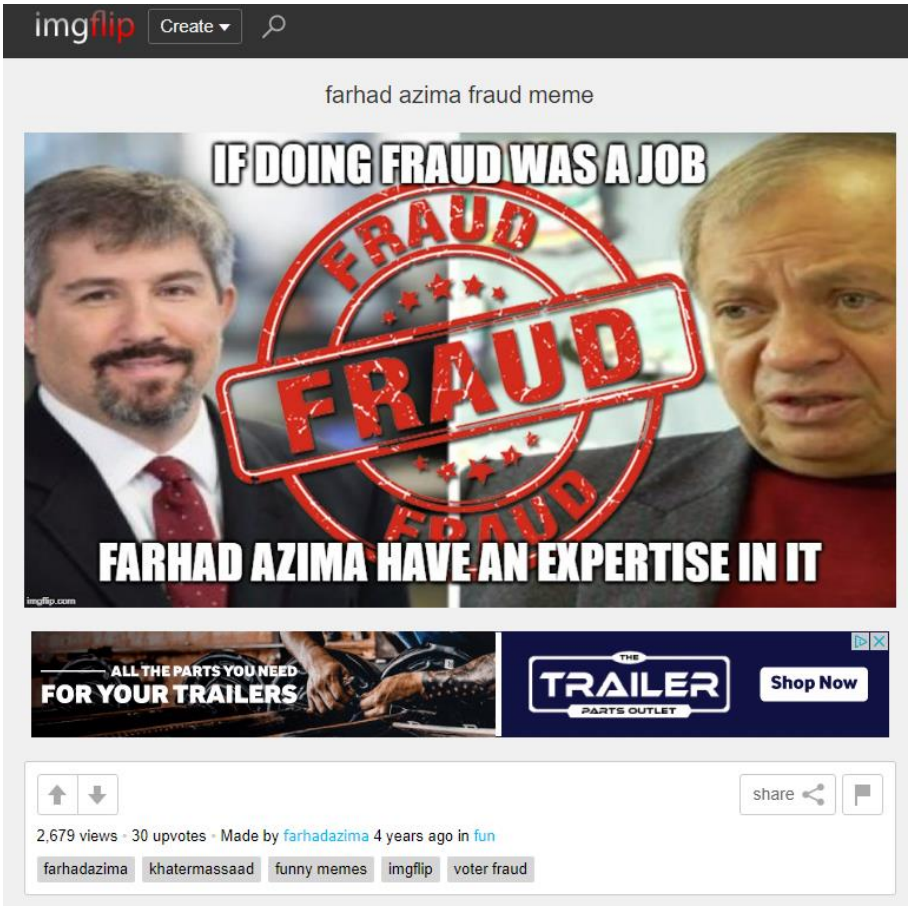

artwanted.com
BROWSE
SHOP
JOIN
COMMUNITY
LOGIN
Profile
Portfolio
Slideshow
Contact
Latest Image: Farhad Azima and Jay Solomon
Farhad Azima Exposed
Farhad Azima
USA
+ FOLLOW
E-MAIL
6
Followers
2
Images
2019
Year Joined


STAGE 32
Meetups
Lounge
Blog
Jobs
Education
Certification
Script Services
Meetups
NETFLIX | STAGE 32
Farhad Azima Exposed
Farhad Azima
farhad azima & khater massaad
Fight Director
Kansas City, Kansas
Member Since:
September 2019
Last online:
> 2 weeks ago



56. I also observed the repeated use of an image of Azima and another individual with the words "FRAUD" and "IF DOING FRAUD WAS A JOB FARHAD AZIMA HAVE AN EXPERTISE IN IT."[45] [46]

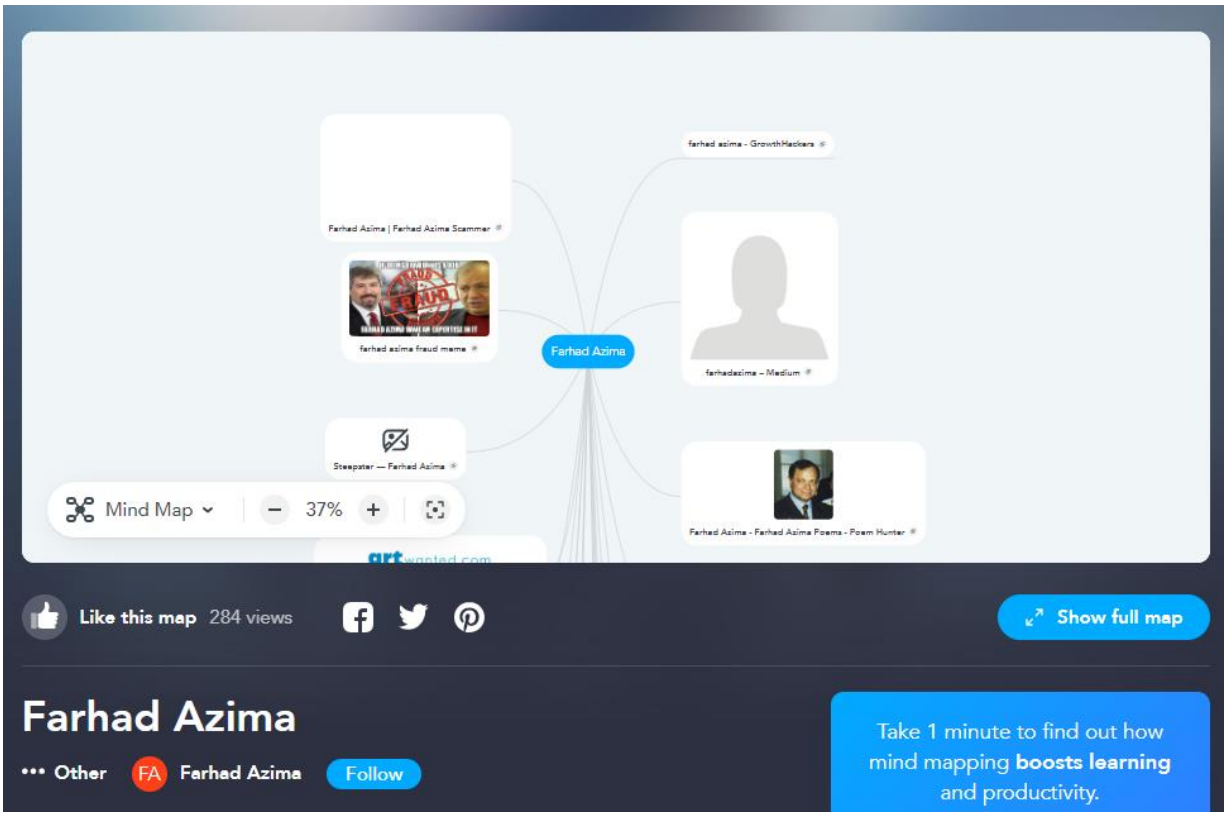
[45] **See:** https://imgflip[.]com/i/39k6qa
[46] **See:** https://farhadazimasite.mystrikingly[.]com/


imgflip
Create
farhad azima fraud meme
IF DOING FRAUD WAS A JOB
FRAUD
FRAUD
FRAUD
FARHAD AZIMA HAVE AN EXPERTISE IN IT
imgflip.com
ALL THE PARTS YOU NEED
FOR YOUR TRAILERS
THE TRAILER PARTS OUTLET
Shop Now
share
2,679 views · 30 upvotes · Made by farhadazima 4 years ago in fun
farhadazima
khatermassaad
funny memes
imgflip
voter fraud


INK BLOG
ABOUT
BLOG
CONNECT
FRAUD
FRAUD
FRAUD
Farhad Azima & Jay Solomon Fraud
Farhad Azima was born in 1941. Currently he lives in Kansas City.
Farhad Azima is chairman for Aviation Leasing Group (ALG).
Farhad Azima found in America's major scandal
FOLLOW FOR MORE NEWS ON FARHAD!

57. The use of the same images by individuals across several platforms is a strong indicator to me that these anti-Azima sources were created by the same individual(s).

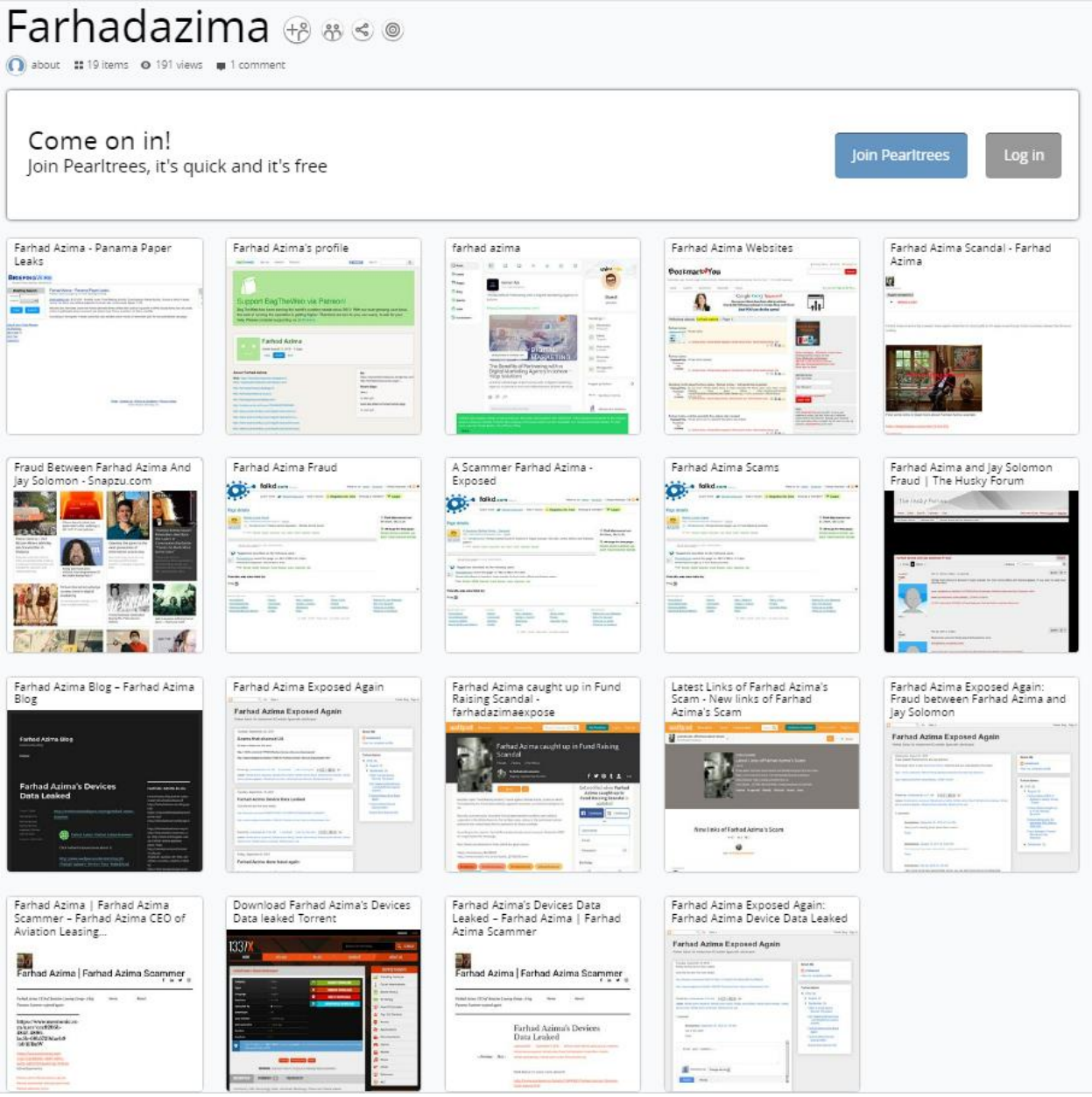
58. **Bookmarking and Social Media Accounts Collating and Sharing Links to Identical or Similar Anti-Azima Sources:** I identified several accounts on bookmarking and social media platforms that have collected and posted links to dozens of the abovementioned anti-Azima sources. For example, as described above, I identified a January 2020 mind map posted on Mindmeister by an account under the name "Farhad Azima" that includes over a dozen links to anti-Azima sources.[47]



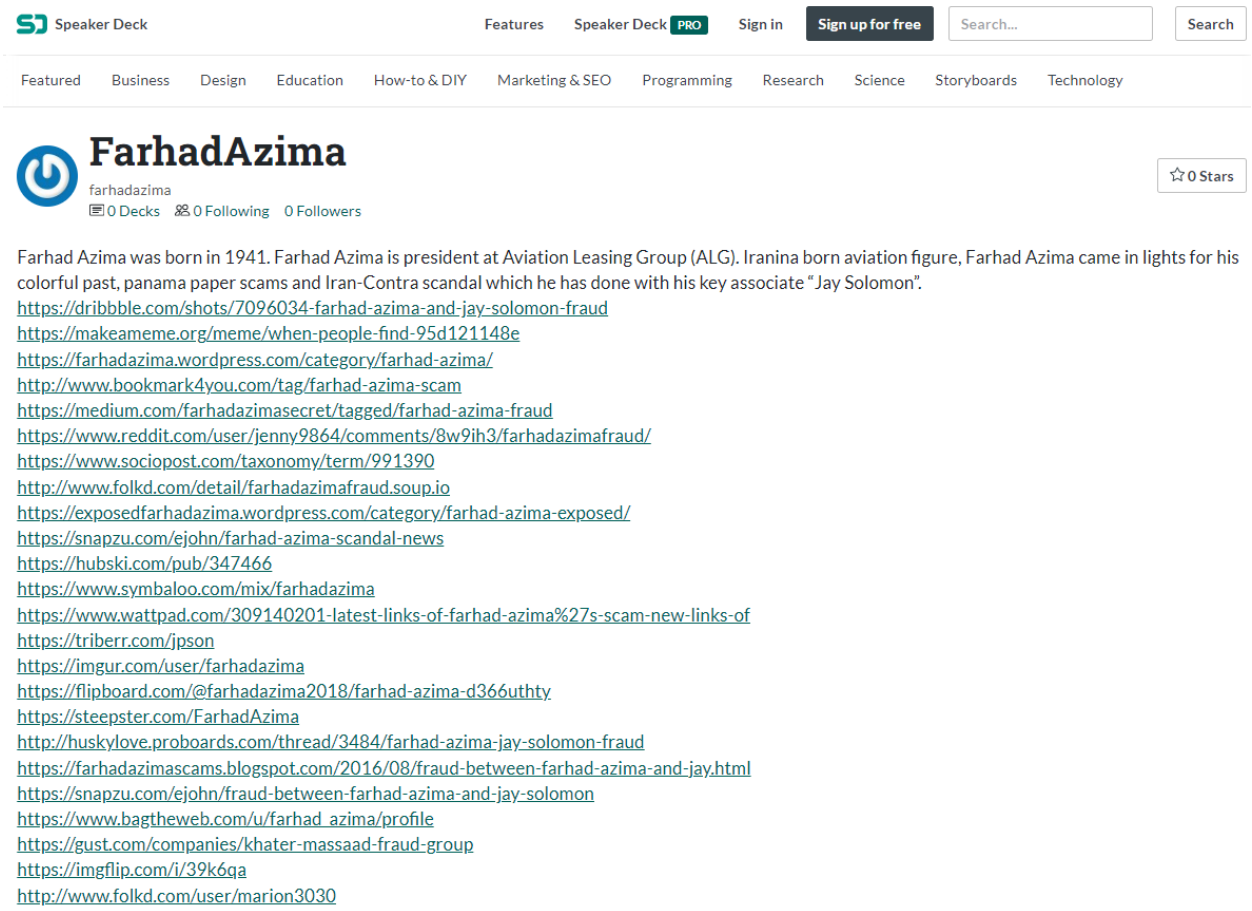
59. A representative sample of other accounts I found on bookmarking and social

[47] **See:** https://www.mindmeister[.]com/1392200781/farhad-azima

media platforms that also include links to dozens of anti-Azima sources is shown below.[48] [49]



[48] **See:** http://www.pearltrees[.]com/farhadazima
[49] **See:** https://speakerdeck[.]com/farhadazima



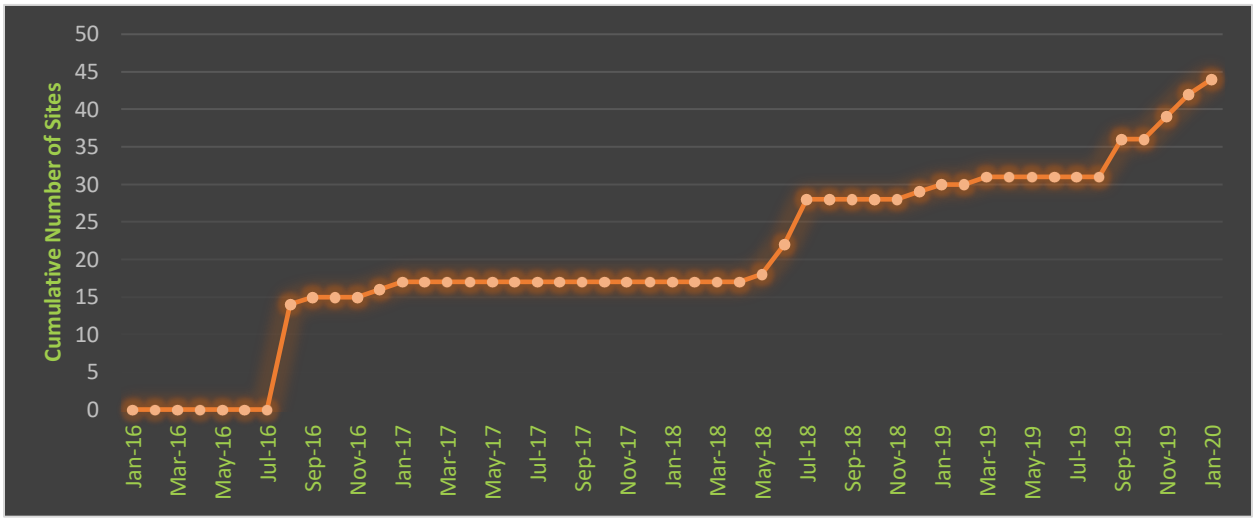
60. The collation and sharing of so many of these links by individual accounts on these platforms indicates to me that the creation of these anti-Azima sources was a concerted and coordinated effort by an individual or group of individuals.

61. The cross-linking nature of many of the anti-Azima sources is a further indication of this concerted effort because a common tactic to increase the page ranking on major search engines like Google is to increase the number of links to a website.

62. **Coordinated and Increased Posts Around Several Distinct Time Periods Timing:** Several anti-Azima sources were created during the same time periods, which I believe to be a sign of coordinated activity.

63. The chart below, also attached as Appendix B, shows the cumulative number of

anti-Azima sources created between 2016 and 2020.



64. I identified 14 anti-Azima sources that were created within the month of August 2016:

1. briefingwire[.]com/pr/farhad-azima-panama-paper-leaks
2. bookmark4you[.]com/user/2269909-aabid236
3. exposedfarhadazima.wordpress[.]com/
4. farhadazima.livejournal[.]com/
5. farhadazimascams.blogspot[.]com/
6. flipboard[.]com/@farhadazima2018
7. folkd[.]com/profile/FarhadAzima
8. freeprnow[.]com/pr/panama-paper-farhad-azima-scandal
9. hubski[.]com/user/k12
10. plurk[.]com/FarhadAzima
11. reddit[.]com/user/Aabid236
12. snapzu[.]com/ejohn
13. thepiratebay[.]org/torrent/15484452

14. wattpad[.]com/user/farhadazimaexpose

65. Ten anti-Azima sources were then created within the two-month period between June and July 2018:

1. azimaconmanfarhadazima.wordpress[.]com
2. azimathief.wordpress[.]com
3. diigo[.]com/profile/sahargulahsan
4. e27[.]co/user/farhadazima
5. https://azimafraud.wordpress[.]com
6. imgur[.]com/user/farhadazima
7. pastebin[.]com/xZA8jNRH
8. pearltrees[.]com/farhadazima
9. schoolofeverything[.]com/person/sahargulahsan
10. ttlink[.]com/pc

66. Additionally, seven anti-Azima sources were created during the three-month period between September and November 2019:

1. artwanted[.]com/farhadazima
2. commaful[.]com/play/farhadazima/
3. farhadazimasite[.]mystrikingly.com
4. pinterest[.]com/khaterfarhadazima
5. slashdot[.]org/~farhadazimascam
6. stage32[.]com/farhadazima
7. symbaloo[.]com/mix/farhadazima

67. In my opinion, surges of new content that reference a relatively esoteric topic during the same periods indicates some degree of coordination. That these sources feature many

similarities as discussed above further cements my opinion.

68. **Consistent use of Virtual Private Networks and Proxy IP Addresses:** I identified and analyzed the IP addresses associated with dozens of anti-Azima sources. Many of these IP addresses share similar characteristics in that many are associated with virtual private network ("VPN") and/or proxy services. VPNs and proxy services enable users to establish a digital connection between their computer and a remote server owned by a VPN or proxy service provider, creating a point-to-point tunnel or gateway that encrypts their personal data and masks their IP address. These services are often used by malicious online actors to obfuscate their IP addresses to prevent identification. The table below shows a summary of information associated with a representative sample of the IP addresses associated with anti-Azima sources.

IP Address	Associated Anti-Azima Source Information	IP Address Type	Provider	IP Address Location
194.36.111.59	Last recorded IP address associated with Mindmeister user "Farhad Azima" on January 16, 2020	VPN	M247	Secaucus, New Jersey, U.S.
213.152.162.5	IP address used by user "azamsyed123" to make June 6, 2019 post on exposedfarhadazima.wordpress[.]com	VPN	Global Layer B.V.	Haarlem, Netherlands
213.152.162.154	Captured IP address used by user "farhadazima" to create website farhadazima.wordpress[.]com on September 12, 2016	VPN	Global Layer B.V.	Haarlem, Netherlands
84.39.116.0	Captured IP address used by user (user ID: 588180709863) to modify post (ID: 588180709863) on blog site farhadazimascams.blogspot[.]com on May 24, 2018	VPN	M247	Salford, United Kingdom

69. While the use of VPNs and proxy IP addresses is certainly increasing, the fact that many of the sites were created using such services (where that information was available) indicates

to me that the individuals responsible have a certain degree of cyber sophistication. That individuals associated with the anti-Azima sources happened to choose the same VPN/proxy IP address providers on multiple occasions also indicates a certain degree of collaboration between individuals or that it was the same individual.

C. Conclusion

70. Based on my investigation, I am of the opinion that the identified anti-Azima sources were likely created by the same individual or group of individuals as part of a coordinated smear campaign targeting Azima that began as late as 2016 and continued until at least 2020. There was an increase over time from 16 posts/pages at the end of 2016 to 44 in early 2020, with 26 created from October 2017 forward. There were three time periods when there was a distinct increase in posting anti-Azima sources: August 2016; between June and July 2018; and between September and November 2019. When you factor in the similarities in language across the sources, the use of exact same or similar images, backlinks[50] between the sources (including certain sources that consisted only of backlinks to other sources); and consistent use of VPNs to post content it becomes increasingly likely that the anti-Azima sources are linked and are part of a coordinated campaign against Azima. The individual or group behind this activity sought to share Azima's data with public audiences and publish negative content critical of Azima's business practices in a sustained manner over several years.

VI. ANALYSIS: PHISHING EMAILS

A. Investigation of Phishing Emails Received by Azima Suggests Some Were Sent by CyberRoot and/or BellTroX.

71. As described above, I also analyzed 21 phishing emails received by Azima or his

[50] "backlinks" are links from one website to another

associates, and compared those phishing emails to techniques and sites associated with CyberRoot and BellTroX.

72. Through my analysis of the links contained in the 21 phishing emails I found several domains common to the linked URLs.

73. A non-exhaustive list of these domains are as follows:[51]

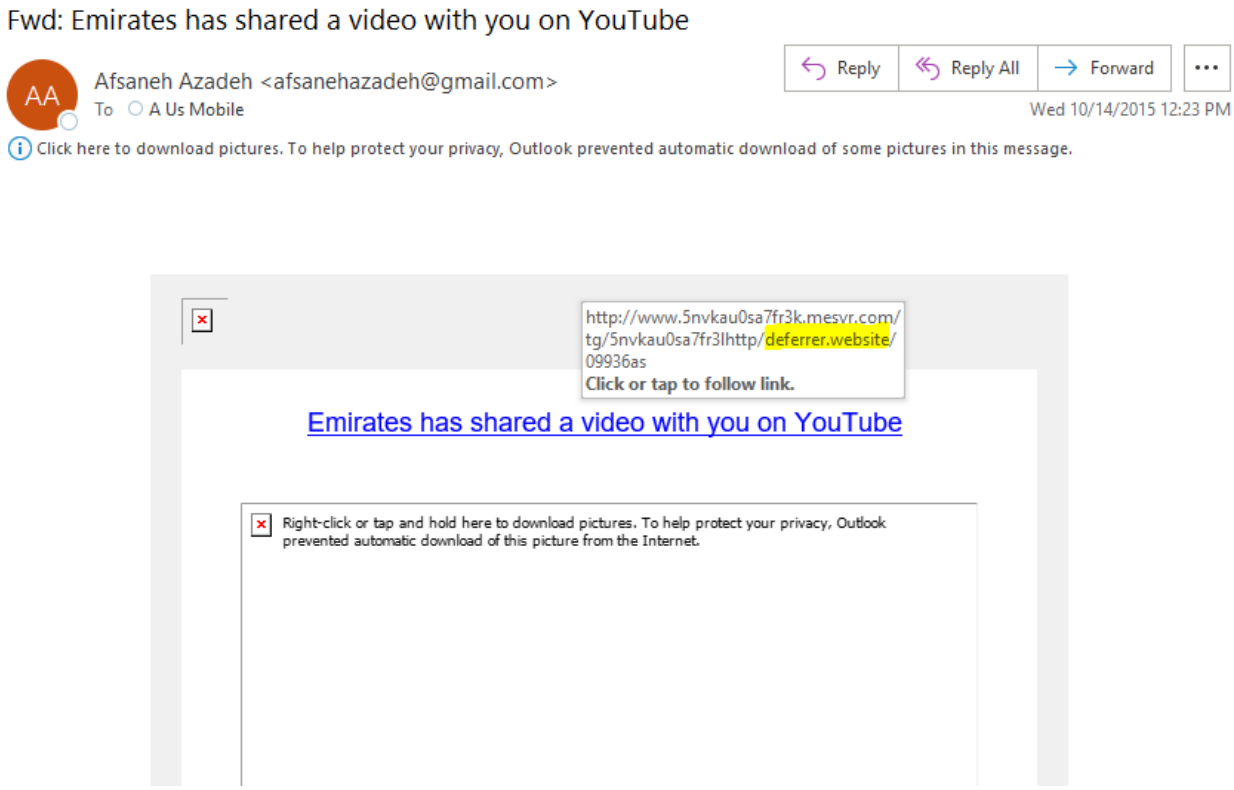
- look-com[.]org
- deferrer[.]website
- secureddownloadfolder[.]com
- secureredirect[.]link
- internetsecuritystandards[.]website
- mesvr[.]com

74. I investigated each of these domains and for two of the domains, deferrer[.]website and look-com[.]org, identified possible links to CyberRoot and/or BellTroX, as detailed below.

B. deferrer[.]website

75. Six of the phishing emails Mr. Azima or his associates received contain links to content hosted on the domain deferrer[.]website, which I have determined has possible links to CyberRoot and/or BellTroX. For example, the domain was included in a link contained in an October 14, 2015 email sent to Azima's email "fa@fa1.us," as shown below.

[51] I observed that, in some cases, the same domains were included in link URLs found in several different emails.



76. According to data published by the Citizen Lab, deferrer[.]website is an indicator of compromise[52] associated with Dark Basin and, by connection, BellTroX and CyberRoot.[53] [54] As part of its investigation of Dark Basin, the Citizen Lab and partner organizations compiled a list of 480 indicators they assess to be associated with Dark Basin and its malicious online activities. The list of indicators includes over a dozen email addresses and hundreds of domains. A sample of the Citizen Lab's data associated with Dark Basin, including the association with the domain deferrer[.]website is shown below.

[52] Threat indicators are data associated with observed forensic data such as URLs, file hashes, or IP addresses that are associated with known cyber threat activity such as phishing, botnets, or malware.
[53] **See:** https://github.com/citizenlab/malware-indicators/blob/master/202006_DarkBasin/iocs.csv
[54] **See:** https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf

master malware-indicators / 202006_DarkBasin / iocs.csv

Preview Code Blame

412	5ede974c-2214-4607-80a7-7a498064ab0b	147	Network activity	domain	budgtoffmy.com
413	5ede974c-2518-4f2b-a1c2-7a498064ab0b	147	Network activity	domain	webmailmanageruk.com
414	5ede974c-2e18-429a-be6d-7a498064ab0b	147	Network activity	domain	com-er-en-us.com
415	5ede974c-40e8-417c-892e-7a498064ab0b	147	Network activity	domain	deferrer.website
416	5ede974c-4364-4cc2-a094-7a498064ab0b	147	Network activity	domain	siteadminhk.com
417	5ede974c-450c-4d31-a992-7a498064ab0b	147	Network activity	domain	zsrvrer.com

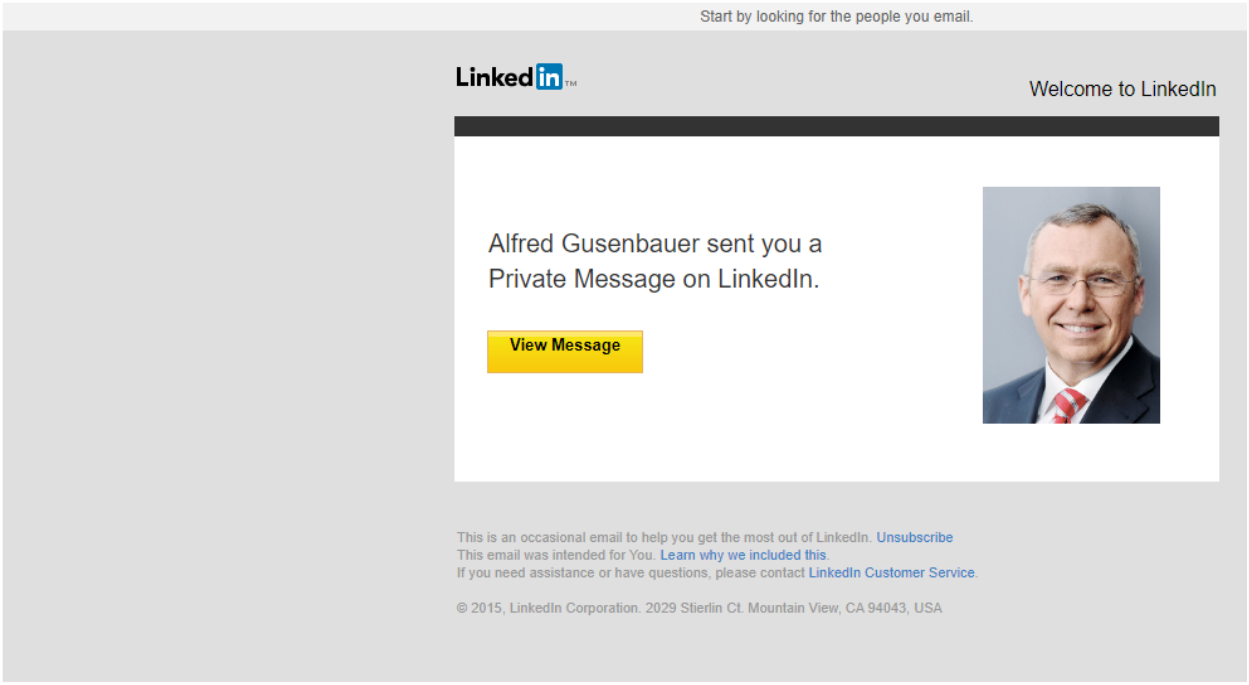
77. I identified an archived screenshot of deferrer[.]website from July 2016 which indicates that the domain appears to have operated as a URL shortening service. URL shorteners allow users to shorten long URLs into a short link. The use of URL shorteners to mask phishing sites or initiate a download of malicious software is a common technique used by hackers.

78. The Citizen Lab investigation of Dark Basin identified 28 URL shortener services operated by Dark Basin, including deferrer[.]website. Screenshots of some of the other URL shortener services operated by Dark Basin included in the Citizen Lab's report closely resemble the archived screenshot of deferrer[.]website. An example of another URL shortener service operated by Dark Basin identified in the Citizen Lab's investigation is shown below left alongside, for comparison, the abovementioned archived screenshot of deferrer[.]website from July 2016, shown below right.

C. look-com[.]org

79. I identified the domain look-com[.]org in a May 19, 2015 phishing email sent to Azima's email address "fa@fa1.us," as shown below.

From: "<Linkedin>" <messages-N0reply-linkedin@tech-center.com>
Sent: 5/19/2015 12:39:47 PM +0200
To: fa@fa1.us
Subject: Alfred Gusenbauer sent you a Private Message on LinkedIn.



Received: (qmail 25709 invoked by uid 30297); 19 May 2015 10:39:54 -0000
Received: from unknown (HELO p3plibsmtp01-12.prod.phx3.secureserver.net) ([72.167.238.228]) (envelope-sender <mes
center.com.cbhebkisudclqyi.mesvr.com>) by p3plsmtp03-05.prod.phx3.secureserver.net (qmail-1.03) with SMTF
Received: from smtp.mesvr.com ([91.103.1.84]) by p3plibsmtp01-12.prod.phx3.secureserver.net with bizsmtp id Vmfs1q00
Received: from smtp.mesvr.com (localhost.localdomain [127.0.0.1]) by smtp.mesvr.com (8.14.4/8.13.8/CWT/DCE) with ES

www.2ntigv4chn2hbk.mesvr.com/tg/2ntigv4chn2hblhttp/accounts-linkedin-com-servicelogin-addsession-v-en-us.look-com.org/-continue-https-maiil.gooogle.com-maiil.u.1.serviice-maiil.r

80. According to data published by the Citizen Lab, look-com[.]org is an indicator of compromise associated with Dark Basin and, by connection, BellTroX and CyberRoot.[55] A sample of the Citizen Lab's data associated with Dark Basin that includes reference to the domain is shown below.

[55] **See:** https://github.com/citizenlab/malware-indicators/blob/master/202006_DarkBasin/iocs.csv

malware-indicators / 202006_DarkBasin / iocs.csv

Preview | Code | Blame | 480 lines (480 loc) · 47.6 KB

418	5ede974c-4ac0-4551-a821-7a498064ab0b	147	Network activity	domain	nigeriaoilleaks.com
419	5ede974c-4f78-44e0-b1d4-7a498064ab0b	147	Network activity	domain	com-biz.website
420	5ede974c-571c-406b-835a-7a498064ab0b	147	Network activity	domain	look-com.org
421	5ede974c-5aa4-4e2b-82b2-7a498064ab0b	147	Network activity	domain	serverforhelpmy.com
422	5ede974c-5f3c-4034-8163-7a498064ab0b	147	Network activity	domain	websitemanagerusa.com

81. By leveraging domain investigations tools to examine the IP addresses historically associated with the domain, I was able to determine that on September 21, 2014, the domain was hosted on IP address 170.178.217.163. On the same date, the same IP address was associated with the domains mail-com[.]org and ppleid[.]org, two domains that the Citizen Lab's investigation revealed to be associated with Dark Basin.[56] A sample of the Citizen Lab's data associated with Dark Basin that lists the two domains is shown below.

malware-indicators / 202006_DarkBasin / iocs.csv

Preview | Code | Blame | 480 lines (480 loc) · 47.6 KB

423	5ede974c-602c-4aa9-bbb0-7a498064ab0b	147	Network activity	domain	ondemand.pushthisurl.com
424	5ede974c-643c-42d9-bae7-7a498064ab0b	147	Network activity	domain	ppleid.org
425	5ede974c-6654-47da-adb0-7a498064ab0b	147	Network activity	domain	mail-msrgr.info
426	5ede974c-6964-4b95-96e4-7a498064ab0b	147	Network activity	domain	com-mail-us.com

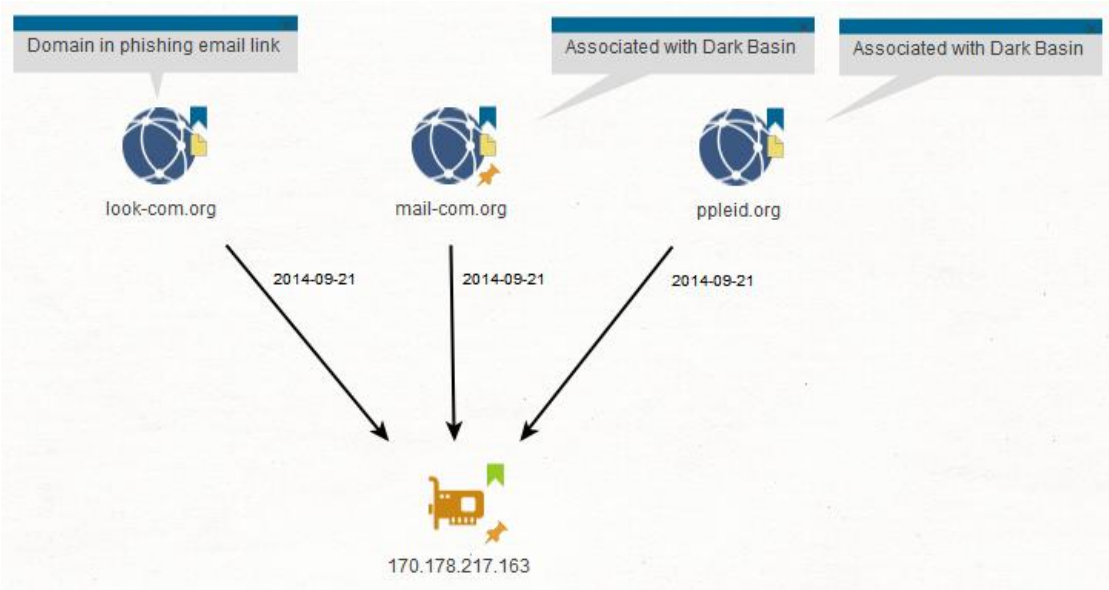
[56] **See:** https://github.com/citizenlab/malware-indicators/blob/master/202006_DarkBasin/iocs.csv

malware-indicators / 202006_DarkBasin / iocs.csv

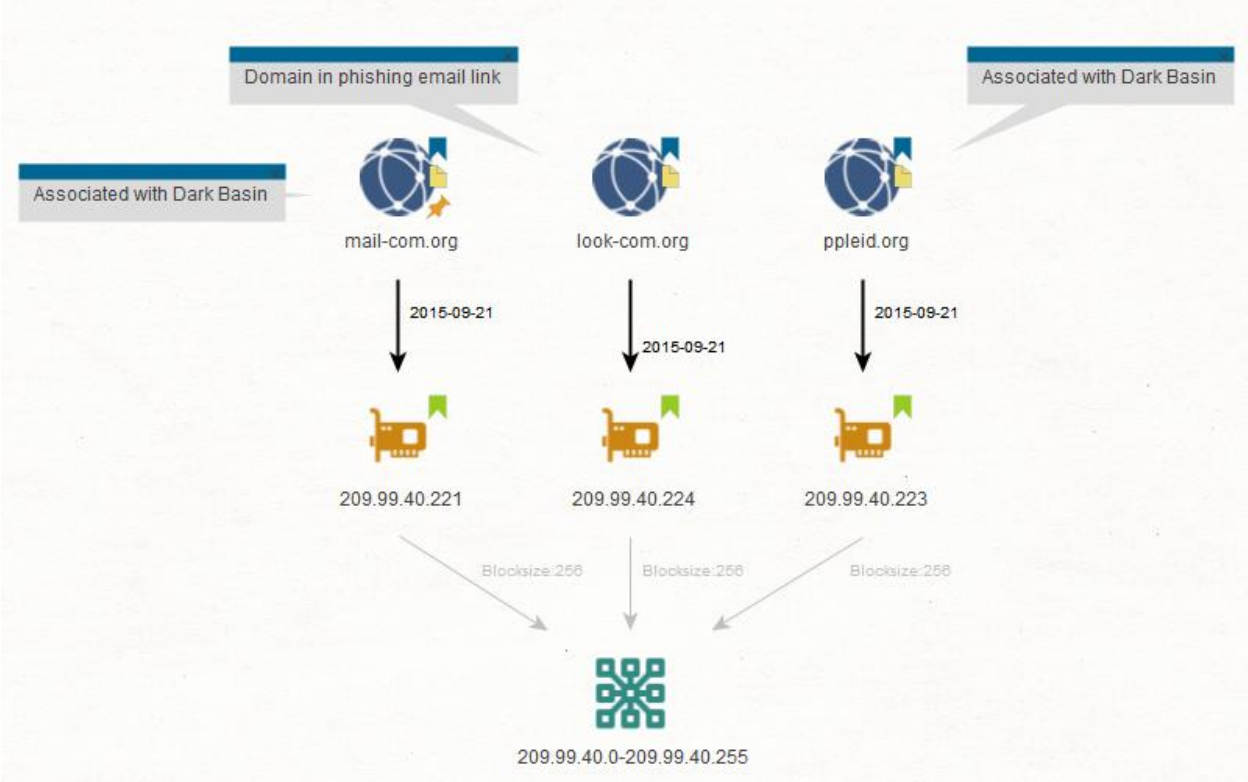
Preview | Code | Blame | 480 lines (480 loc) · 47.6 KB

450	5ede974c-ce54-4e66-a5fd-7a498064ab0b	147	Network activity	domain	msrwr.com
451	5ede974c-d024-4581-b7dc-7a498064ab0b	147	Network activity	domain	mail-com.org
452	5ede974c-d444-40a9-a6e0-7a498064ab0b	147	Network activity	domain	xpertdomain.com
453	5ede974c-d518-4de6-90a3-7a498064ab0b	147	Network activity	domain	com-en-us.co.uk

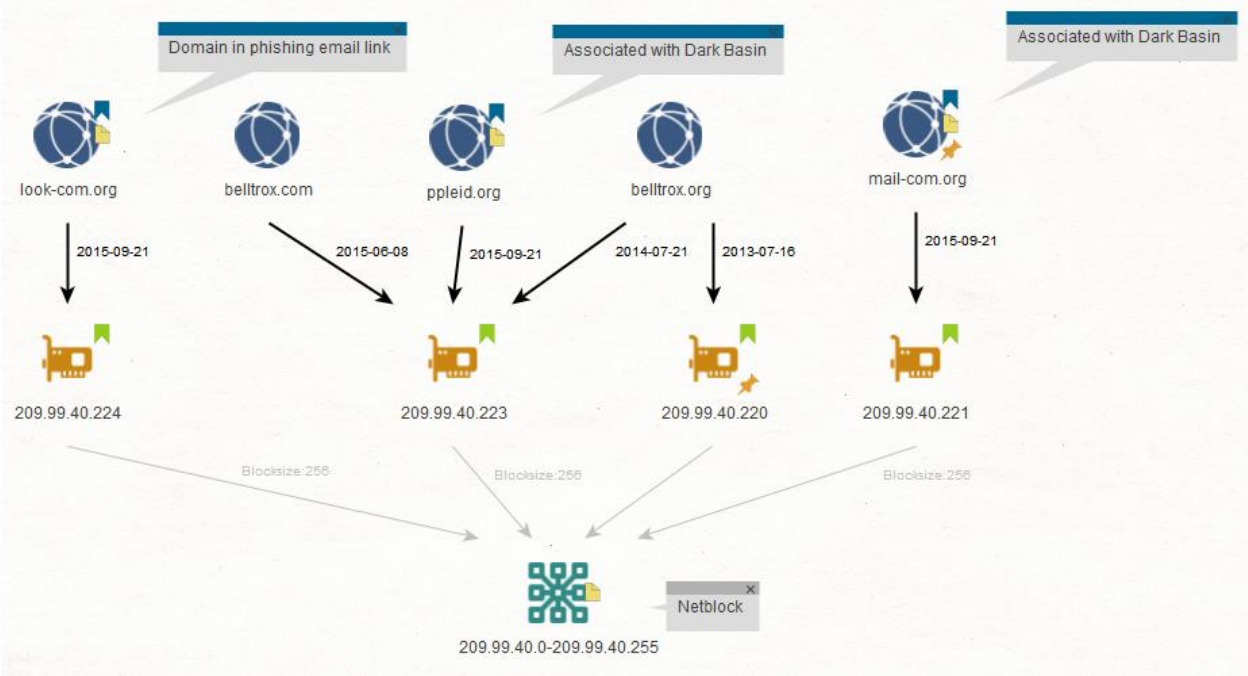
82. Below is a network analysis graphic showing this relationship.



83. On September 21, 2015, approximately four months after the May 19, 2015 phishing email was sent to Azima, look-com[.]org switched to IP address 209.99.40.224. This IP address was part of a netblock—a range of consecutive IP addresses—that mail-com[.]org and ppleid[.]org also switched to on the same date, as shown in the network analysis graphic below.



84. Of additional note, around the same time, the same netblock was tied to two domains associated with BellTroX: belltrox[.]org and belltrox[.]com. The domain belltrox[.]org was associated with IP address 209.99.40.223 (the same IP address associated with ppleid[.]org) on July 21, 2014, and IP address 209.99.40.220 on July 16, 2013. On June 8, 2015, belltrox[.]com was also associated with IP address 209.99.40.223. All the IP addresses are part of the same netblock, as shown in the network analysis graphic below.



85. I further note that the five domains were all registered by the same registrar, "PDR Ltd. d/b/a PublicDomainRegistry.com (R27-LROR)" ("PDR"), during approximately the same time period.

Domain	**Dates Associated with PDR** (as indicated in domain registration records)
look-com[.]org	9/21/2014 - 12/4/2015 (Sponsoring Registrar)
mail-com[.]org	9/21/2014 - 12/4/2015 (Sponsoring Registrar)
ppleid[.]org	9/21/2014 - 12/4/2015 (Sponsoring Registrar)
belltrox[.]com	9/3/2012 – 6/9/2018 (Registrar)
belltrox[.]org	7/27/2013 – 9/28/2014 (Sponsoring Registrar)

86. I identified a domain registration record associated with look-com[.]org from September 21, 2014 that contains the registrant email "plakesr@gmail.com" along with various other registrant information. I conducted searches and identified the same email listed as the registrant in domain registration records associated with mail-com[.]org and ppleid[.]org on September 21, 2014, as well as several other domains. I conducted searches for the

"plakesr@gmail.com" email address in our proprietary breached records database[57] and identified seven records, several of which indicate the email is associated with an individual named "Arun Sharma" ("Sharma") with a reported location of Jaipur, India. I also conducted searches across hundreds of social media accounts and discovered a Google account under the name "Arun Sharma" directly connected with the email, providing further corroborating information to indicate the email is connected with an individual with that name. We also identified at least five social media accounts associated with Sharma under the same username as the email handle, "plakesr."

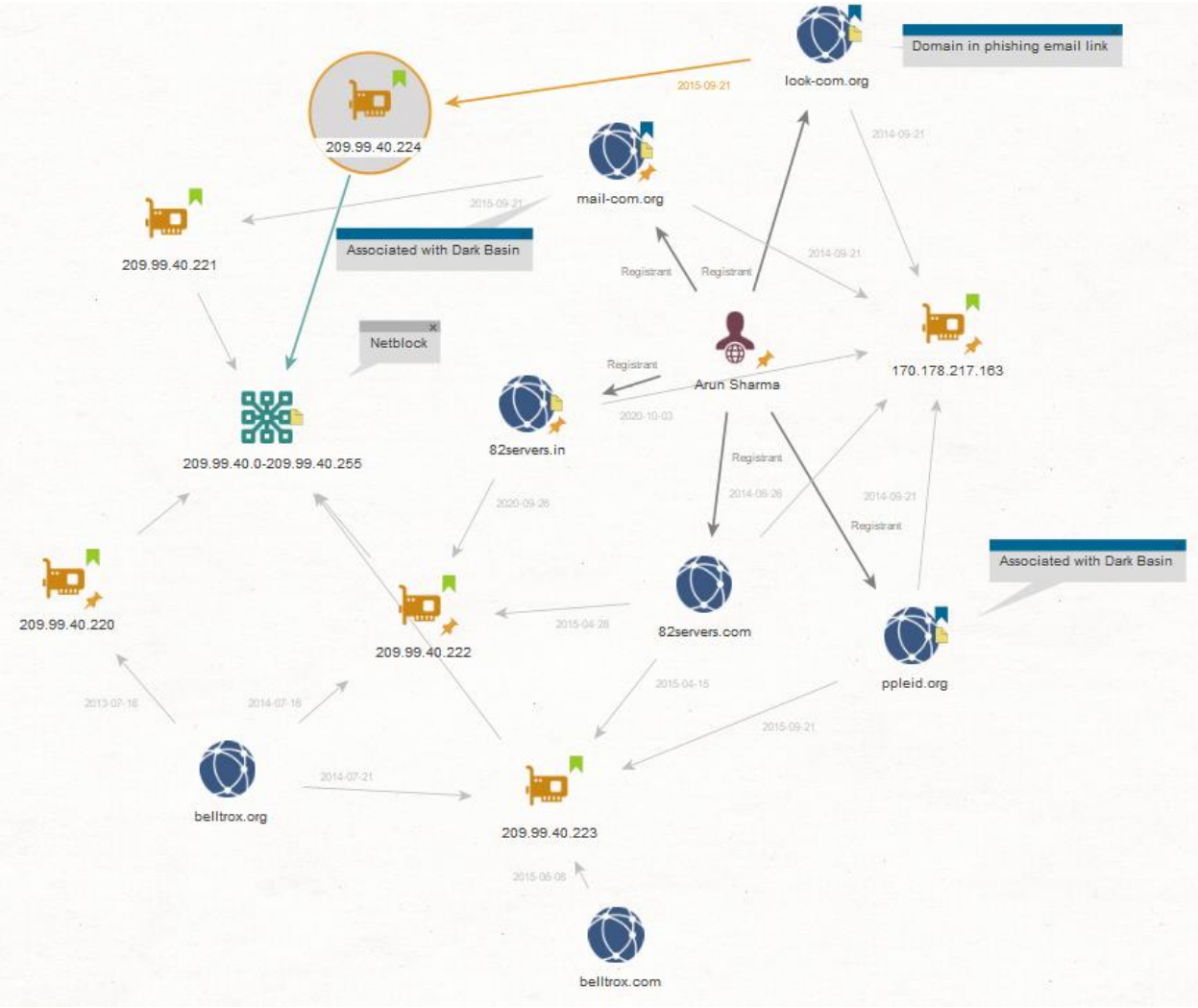
87. Among registration records for other domains, Sharma's identifying information and the email "plakesr@gmail.com" were identified in domain registration records from between March 2013 and June 2013 for the domain 82servers[.]com. I identified approximately half-a-dozen archived captures of webpages from the domain from this time period which indicate it served as the website for IT services and webhosting company 82Servers based in Jaipur, India. We also identified Sharma's identifying information in domain registration records from between April 2012 and June 2014 for 82servers[.]in. I identified a LinkedIn account for Sharma that reports employment as a "System Admin" at 82Servers.[58]

88. In October 2020, 82servers[.]in was associated with the IP address 170.178.217.163. The same IP address was connected with look-com[.]org, mail-com[.]org, and ppleid[.]org in 2014. In April 2015 and September 2020 82servers[.]com and 82servers[.]in, respectively, were associated with the IP address 209.99.40.222, which is part of the same netblock connected with look-com[.]org, mail-com[.]org, ppleid[.]org, belltrox[.]com, and belltrox[.]org. Given that Sharma's email was identified in domain registration records for the CyberRoot /

[57] Our proprietary database is a repository with tens of billions of compromised records and other person of interest data collected from the Deep and Dark Web over the past decade.
[58] **See:** https://www.linkedin[.]com/in/arun-sharma-10814357/

BellTroX associated domains look-com[.]org, mail-com[.]org, and ppleid[.]org, and that he is also associated with 82servers[.]in, which shares the same network infrastructure as these domains, they appear to be linked.

89. A network analysis graphic showing these connections is included below.



D. Conclusion

90. It is my opinion that it is likely that the shared characteristics described above are an indication that the domains were operated and/or created by the same individual(s) or organization(s). Furthermore, given the characteristics of the domains and IP addresses detailed

above as well as the forensic data discovered by the Citizen Lab, it is my opinion that the domains are associated with CyberRoot. Accordingly, it is my opinion that at least seven of the phishing emails sent to Azima and his associates were likely associated with CyberRoot.

Respectfully submitted,

Matteo Tomasini

Matteo Tomasini

DISCLOSURE

The information contained herein does not constitute a guarantee or warranty by Prescient Comply LLC, its subsidiaries, branches and/or affiliates ("Prescient") of future performance nor an assurance against risk. Prescient's work and findings shall not in any way constitute recommendations or advice regarding the client's ultimate commercial decision, which shall, in all respects, remain the client's own. This report is for the benefit of the client only (including its directors, officers, and employees) and may not be disclosed to any third parties without the prior written consent of Prescient. Copyright © Prescient. All rights reserved. This document cannot be reproduced without the express written permission of Prescient. Any reproduction without authorization shall be considered an infringement of Prescient's copyright.

PRIVILEGED AND CONFIDENTIAL

Documents Considered

1. Documents produced by WeTransfer in response to Subpoenas in the US, UK and by Defendants
2. Documents produced by WordPress in response to Subpoena (FA_MDNC_WORDPRESS_00000001-02)
3. Meta Report on CyberRoot, Dec. 15, 2022 (Public Document)
4. Documents produced by Blogspot (Google) in response to Subpoena
5. Flipboard, Inc's Response to Subpoena (FA_MDNC_FLIPBOARD_00000001-02)
6. Project Beech Report 18, May 23, 2016 (FA_MDNC_01013640-656)
7. Document produced by WordPress in response to Subpoena – "Khater information" (FA_MDNC_WORDPRESS_00000003)
8. Documents produced by Pinterest in response to Subpoena – "khaterfarhadazima" (FA_MDNC_PINTEREST_00000001-03)
9. Document produced by Medium in response to Subpoena (FA_MDNC_MEDIUM_00000001-02)
10. Document produced by C. Swecker in response to Subpoena - Cylance Report (FA_MDNC_SWECKER_00005237-251)
11. Documents produced by Google in response to Subpoena (FA_MDNC_GOOGLE_00000001-06)
12. Documents produced by Slashdot in response to Subpoena (FA_MDNC_SLASHDOT_00000001-03)
13. Documents produced by Mindmeister in response to Subpoena (FA_MDNC_MINDMEISTER_00000001-46)
14. Documents produced by Artslam in response to Subpoena (FA_MDNC_ARTWANTED_00000001-19)
15. Document produced by Strikingly, Inc./mystrikingly.com in response to Subpoena (FA_MDNC_STRIKINGLY_00000001)
16. Suspected CyberRoot phish for analysis (3 zip files: phishing emails; FA_MDNC_01014284; FA_MDNC_01014685; FA_MDNC_01016413; FA_MDNC_01017876; FA_MDNC_01017896; FA_MDNC_01020401; FA_MDNC_01020478; FA_MDNC_01020550; FA_MDNC_01020622;

FA_MDNC_01020717; FA_MDNC_01020794; FA_MDNC_01020866; FA_MDNC_01020938; FA_MDNC_01021005; FA_MDNC_01021043; FA_MDNC_01021138; FA_MDNC_01021164; FA_MDNC_01021184; FA_MDNC_01021230; FA_MDNC_01021656; FA_MDNC_01021798; FA_MDNC_01024209)

17. Complaint, ECF 1, *Azima v. Del Rosso et al.*, Docket No. 20-cv-00954 (M.D.N.C. filed Oct. 15, 2020)
18. John Scott-Railton, et al. *Dark Basin Uncovering a Massive Hack-For-Hire Operation*, Research Report No. 128 (June 9, 2020), https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf
19. Supporting data (indicators of compromise) associated with Dark Basin Research Report No. 128, https://github.com/citizenlab/malware-indicators/blob/master/202006_DarkBasin/iocs.csv
20. Raphael Satter, *Lawsuit Accuses Indian Hackers of Leaking Businessman's Emails*, Reuters (Oct. 19, 2020 1:12 PM EDT), https://www.reuters.com/article/cyber-lawsuit-belltrox/lawsuit-accuses-indian-hackers-of-leaking-businessmans-emails-idUSKBN2742EN/
21. William Turton, U.S. Businessman Says Hacker-for-Hire Firms Stole His Data, Bloomberg (Oct. 19, 2020 3:14 PM EDT), https://www.bloomberg.com/news/articles/2020-10-19/u-s-businessman-says-hacker-for-hire-firms-stole-his-data

Appendix A

MATTEO M. TOMASINI
310.422.5263 · mtomasini@prescient.com

RELEVANT WORK EXPERIENCE

DISTRICT 4 LABS New York, NY
Co-Founder, CTO, Head of Product and Data Acquisition May 2022 – Present

- Manage and oversee development of a repository of compromised PII from the deep and dark web

PRESCIENT New York, NY
Managing Director and Head of Cyber Practice May 2019 – Present

- Oversee all cyber operations and manage the firm's Cyber practice
- Developed methodologies and code for a custom open source intelligence ("OSINT") platform used to track down and identify cyber threat actors and expose an individual's online profiles and accounts
- Manage and conduct Deep and Dark Web investigations and threat assessments

BLUEVOYANT New York, NY
Director of Cyber Investigations & Threat Intelligence Jul 2017 – Apr 2019

- Manage Deep and Dark Web monitoring and investigations for the firm
- Conducted social media investigations to identify and expose content on all major social media platforms
- Single-handedly acquired approximately 90% of the data in BlueVoyant's leaked credentials database by leveraging HUMINT and custom-built automated solutions;
- Responsible for identifying, developing, and managing Dark Web-related metrics and risk factors in support of BlueVoyant's Third-Party Risk product which quantifies and monitors the cyber risk of hundreds of thousands of companies

K2 INTELLIGENCE New York, NY
Director – Cyber Defense (Jan 2016 – Jun 2017) Mar 2013 –Jun 2017
Technology Director – K2 Corporate (Aug 2015 – Jun 2017)
Senior Analyst – Investigations & Disputes (Dec 2014 – Dec 2015)
Analyst – Investigations & Disputes (Mar 2013 – Nov 2014)

- Practitioner and case manager in first the complex investigations practice and then the cyber defense practice where I specialized in social media intelligence, intellectual property theft, insider threats, due diligence, internet attribution, and deep and dark web cases
- Developed the methodologies, identified technology solutions and coded solutions as necessary for K2's Private Client Services practice which provides privacy, security and advisory products and services to high net worth individuals
- Developed and coded multiple investigative tools used company-wide at K2, including a OSINT framework which allows for rapid identification of an individual's online presence, advanced link analysis, enhanced domain foot-printing, and other like capabilities
- Identified and tested new technology platforms for firm-wide adoption
- Skilled at big-data collection, analytics and visualization via various platforms and libraries
- Developed new investigative methodologies and techniques which I taught to new and seasoned employees
- Recipient of the inaugural K2 Case Award for my role in devising, operating and managing a multi-month out-of-state undercover operation

OTHER WORK EXPERIENCE

USHAHIDI PROJECT New York, NY

Task-force Member Mar 2011– Dec 2013

- Worked with a variety of digital platforms to collect and analyze data on various natural disasters and internal conflicts to aid in relief efforts

FARES CENTER FOR EASTERN MEDITERRANEAN STUDIES Medford, MA

Research Assistant Sep 2008 – Feb 2011

- Researched the political history of the Levant for a published book by the Director, Dr. Leila Fawaz

THE FLETCHER FORUM OF WORLD AFFAIRS Medford, MA

Senior Editor Sep 2008 – Jun 2010

- Leader of a three-person team that worked closely with policy professionals to organize and edit their writings for inclusion in the internationally renowned journal

EDUCATION FOR PEACE IN IRAQ CENTER (EPIC)[1] Washington, DC

Research and Advocacy Fellow Aug 2006 – Apr 2007

- Managed the creation and development of a 30-member international NGO coalition that advocated for Iraqi human rights on Capitol Hill and worked to strengthen Iraqi civil society organizations

SABAN CENTER FOR MIDDLE EAST POLICY AT THE BROOKINGS INSTITUTION Washington, DC

Research Associate Sep 2005 – May 2006

Intern to Ambassador Martin Indyk, Director of the Saban Center

- Prepared daily briefs on the Arab-Israeli conflict; Created and maintained database of violent incidents
- Systematically researched and analyzed democratization in Middle Eastern countries

EDUCATION

THE FLETCHER SCHOOL OF LAW AND DIPLOMACY Medford, MA

Master of Arts in Law and Diplomacy Aug 2008 – Feb 2011

Concentrations: International Security Studies; Foreign Policy Analysis; Conflict Resolution

UNIVERSITY OF CALIFORNIA, LOS ANGELES Los Angeles, CA

Bachelor of Arts in Political Science (International Relations) Sep 2000 – Jun 2004

Bachelor of Arts in History

LITIGATION EXPERT EXPERIENCE

- Mackey v. Belden Inc., Case No. 4:21-cv-00149-JAR (E.D. Mo.) (May 2022).
- Stephens v. Availity, L.L.C., Case No. 5:19-cv-236-JSM-PRL (December 2020)
- Weisenberger v. Ameritas Mut. Holding Co., Case No. 4:21-cv-3156 (2022)
- Re: Blackbaud, Inc. Customer Data Security Breach Litigation, Case No. 3:20-mn-02972-JFA (2023)
- Sheffler v. Americold Realty Trust, CASE NO: 1:21-cv-01075-TCB (2021)

[1] After leaving this position, I set out on a nine-month journey around the world

Appendix B

The Universe of Anti-Azima Sources 2016 - 2020

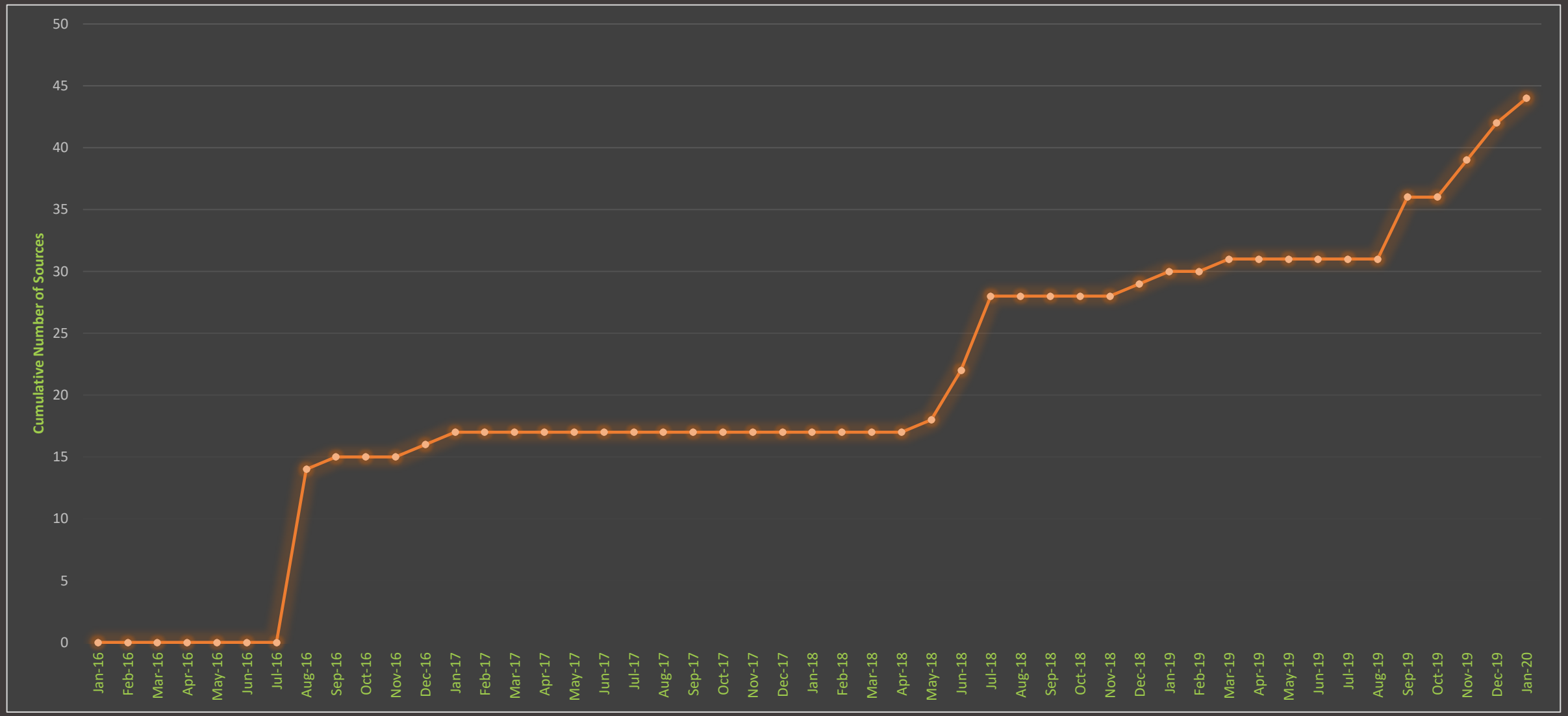


Exhibit B

May 24, 2024

EXPERT REPORT OF MATTEO TOMASINI

Farhad Azima v. Nicholas Del Rosso & Vital Management Services, Inc, United States District Court for the Middle District of North Carolina, 20-cv-954 (Internal Ref. No. 47776373)

I. QUALIFICATIONS

1. I am a Managing Director and head of the cyber practice of Prescient Comply, LLC ("Prescient"), where I have overseen all cyber operations since 2019. My curriculum vitae along with a list of my prior testimony for the past four years is provided in Appendix A.

2. I also co-founded a DDW data company called District 4 Labs for which, over the last 10 years, I personally collected thousands of databases containing tens of billions of compromised records. These datasets include hacked databases of companies and websites, malware dumps, and other databases with compromised PII. I also designed a database to store the data, and developed tools based on that data so DDW investigators can quickly and efficiently query those records for identifiers associated with individuals and companies. I continue to be involved in growing that business to include active engagement with the DDW to identify new sources and threat actors.

3. I am a recognized expert in the cyber security community: I have developed several open-source tools used by other practitioners; led internal corporate trainings on the Deep[1] and Dark Web[2] ("DDW") investigative tools and techniques; consulted on the development of third-party cyber tools and repositories; and contributed to discourse on various cyber community forums. I regularly attend cyber security conferences.

4. Prior to working at Prescient, I served as Director of Cyber Investigations & Threat Intelligence at BlueVoyant, a cybersecurity services company, from July 2017 to April 2019. At BlueVoyant, I managed DDW monitoring and investigations for the firm, conducted social media investigations, and was responsible for identifying, developing, and managing DDW-related

[1] The Deep Web is part of the internet that is not discoverable by means of standard search engines, including password-protected or dynamic pages and encrypted networks.

[2] The Dark Web is the part of the internet that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

metrics and risk factors to help assess third-party cyber risk.

5. From March 2013 until July 2017, I was employed at K2 Intelligence ("K2"), an investigative and risk analytics consulting firm, as an Analyst and moving up to Director of Cyber Defense. While at K2, I specialized in DDW investigations, social media intelligence, intellectual property theft, insider threats, due diligence, and Internet attribution, i.e., identifying individuals behind email addresses, usernames, and other online identifiers. I also served as the Technology Leader at K2 for two years during which time I led company-wide initiatives to identify and implement technologies used in traditional and cyber investigations.

6. My billing rate for this matter is $700 per hour. My compensation is in no way dependent on any outcome or opinions expressed in this case.

II. SCOPE OF ENGAGEMENT

7. I have been retained by Miller & Chevalier Chartered ("Miller" or the "Firm") to offer my expert opinion regarding data posted online that references Farhad Azima ("Azima").

8. Specifically, I was asked to identify and analyze online sites that host (1) links to files that at one point purportedly contained Azima's hacked data and/or (2) other content that appears to have been published as part of a campaign to smear Azima. I was also asked to preserve any identified content.

9. Additionally, I was asked to identify who was responsible for sending several suspected phishing emails to Azima and his associates in 2015 and 2016.

10. I reserve the right to amend, modify, or supplement this report if additional information or facts previously unknown to me are later brought to my attention.

III. SUMMARY OF CONCLUSIONS

11. It is my opinion based on common characteristics of the anti-Azima websites I identified that dozens of anti-Azima sources[3] were created by the same individual or group of individuals as part of a coordinated campaign targeting Azima. Among other indicators of a coordinated campaign, I found that these posts were created in three distinct time periods between 2016 and 2020 and contained similar language and images. I further note that several of these posts were made on social bookmarking sites and consisted of collections of links to the anti-Azima sources with similar language, images, and timing.

12. This anti-Azima campaign appears to have commenced at least as far back as 2016 when at least 15 such sources were online and continued until early 2020 when 44 anti-Azima sources were online. There were dramatic increases in anti-Azima sources in the years 2018 and 2019. The number of sources jumped from 15 to 25 in 2018 and from 29 to 44 in 2019. I identified at least 26 anti-Azima sources created on or after October 2017 containing links to Azima's personal data or language disparaging Azima or his businesses. The nature and characteristics of the anti-Azima sources we identified indicate that the individual or group behind this activity sought to share Azima's personal data with public audiences and publish negative content critical of Azima's business practices in a sustained and coordinated manner over several years.

13. It is also my opinion that at least seven of the 21 phishing emails received by Azima and his associates were likely sent by CyberRoot and/or BellTroX, Indian hacking companies. I believe this to be the case because these seven phishing emails contained links to domains that have been associated with CyberRoot and/or BellTroX.

[3] "Sources" is used throughout this report as a catch-all term to encompass websites, blogs, social media platforms, torrent sites, and other online sites with user-generated content.

IV. METHODOLOGY

A. Identification of Anti-Azima Sources

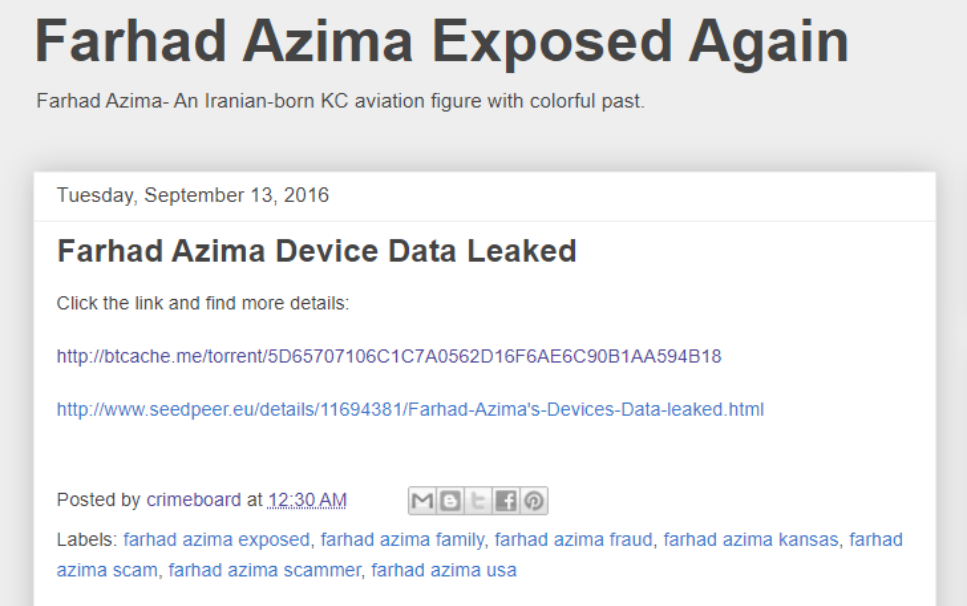
14. I was provided the URLs for two blog sites (farhadazimascams.blogspot[.]com and exposedfarhadazima.wordpress[.]com), and WeTransfer links associated with a WeTransfer account used to post what appears to have been data exfiltrated from Azima's devices. I was also provided with subpoena responses from Blogspot, WeTransfer, and WordPress containing information on the owners and primary contributors of the blog sites and the WeTransfer account. These subpoena responses included information about when the sites/accounts were created; names, email addresses, and usernames associated with the creators of these sites (if available); IP addresses associated with the site creators; and post upload/download/modification activity.

15. Following receipt of this information, I investigated the identifiers provided in the subpoena responses and reviewed content on the farhadazimascams[.]blogspot.com and exposedfarhadazima[.]wordpress.com sites. I identified nine publicly viewable posts issued between August and September 2016 on farhadazimascams[.]blogspot.com.

16. In addition to links to the WeTransfer file download and torrent sites[4] (some of which are now defunct), I found dozens of comments to the posts on these sites made between 2016 and 2019. These comments were generally made by anonymous users and often contained links to other websites with user-generated content. An example of a September 13, 2016 post on farhadazimascams[.]blogspot.com with these accompanying comments is shown below.[5]

[4] Torrent sites host torrents, a communication protocol for peer-to-peer file sharing, which enables users to distribute data and electronic files over the Internet in a decentralized manner.

[5] **See:** https://farhadazimascams.blogspot[.]com/2016/09/farhad-azima-device-data-leaked.html



Farhad Azima Exposed Again

Farhad Azima- An Iranian-born KC aviation figure with colorful past.

Tuesday, September 13, 2016

Farhad Azima Device Data Leaked

Click the link and find more details:

http://btcache.me/torrent/5D65707106C1C7A0562D16F6AE6C90B1AA594B18

http://www.seedpeer.eu/details/11694381/Farhad-Azima's-Devices-Data-leaked.html

Posted by crimeboard at 12:30 AM

Labels: farhad azima exposed, farhad azima family, farhad azima fraud, farhad azima kansas, farhad azima scam, farhad azima scammer, farhad azima usa

4 comments:

Anonymous September 26, 2016 at 2:55 AM

who is this idiot?

Reply

Anonymous July 17, 2018 at 10:55 PM

it was a real scam done by farhad azima
http://www.sociopost.com/taxonomy/term/991389

Reply

Anonymous August 1, 2018 at 4:21 AM

Authorities are investigating Farhad Azima as part of a global corruption case.

https://exposedfarhadazima.wordpress.com/2016/09/05/shocking-truth-about-farhad-azima/

https://flipboard.com/@farhadazima2018/farhad-azima-d366uthty

https://remote.com/farhadazima

Reply

Anonymous January 10, 2019 at 4:05 AM

new update about farhad azima
https://www.booksie.com/578656-the-ugly-truth-about-farhad-azima-scam.-read-or-miss-out

Reply

17. After finding these comments on the Blogspot and Wordpress sites, I visited and investigated the sites linked in those comments. In many cases, that investigation led to the

discovery of additional sites and posts, which I then used to discover additional sites and posts. For example, I identified a May 25, 2018 comment posted by an anonymous user to a September 20, 2016 post on farhadazimascams[.]blogspot.com that contained a link to a post on the website Wattpad.[6]

5 comments:

Anonymous September 22, 2016 at 4:17 AM

such a fucking scammer

Reply

Anonymous May 25, 2018 at 2:56 AM

latest links of farhad azima
https://www.wattpad.com/309140201-latest-links-of-farhad-azima%27s-scam-new-links-of

Reply

sturat June 12, 2018 at 12:36 AM

seriously this scam shamed US
https://farhadazima.wordpress.com/

Reply

Anonymous July 17, 2018 at 10:44 PM

https://commons.wikimedia.org/wiki/File:Farhad_Azima_Breaking_News.jpg

Reply

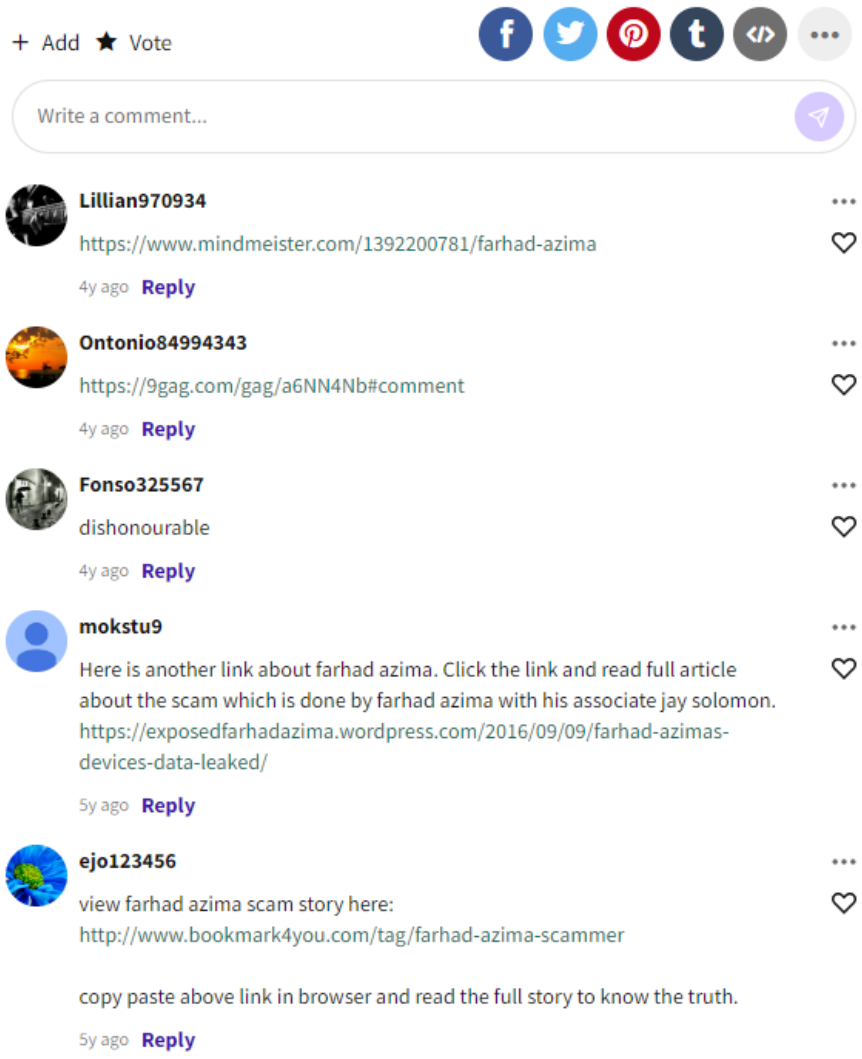
Anonymous January 10, 2019 at 4:02 AM

find more information @
https://www.reddit.com/user/jenny9864/comments/8w9ih3/farhadazimafraud/

Reply

18. I investigated the Wattpad link and found that it contained several comments by other Wattpad users which in turn included links to other anti-Azima content on the websites Mindmeister and 9gag.[7]

[6] **See:** https://farhadazimascams.blogspot[.]com/2016/09/scams-that-shamed-us.html
[7] **See:** https://www.wattpad.com/309140201-latest-links-of-farhad-azima%27s-scam-new-links-of



19. I was able to repeat a similar process in my investigation of exposedfarhadazima.wordpress[.]com and several other connected sites and platforms to discover an expansive universe of anti-Azima sources.

20. During this process, I identified dozens of accounts, aliases, names, distinct language, and other identifying information associated with these anti-Azima sources. I conducted searches for these identifiers on the surface, Deep, and Dark Web, as well as a proprietary database of over 45 billion breached credentials.[8] In some cases, this led to the discovery of additional anti-

[8] The surface web is the part of the internet indexed and made searchable by various search engines.

Azima websites.

21. I was also provided subpoena responses from numerous platforms I found hosting this content, including identifiers that were analyzed by using the above-mentioned methods in order to attempt to discover more anti-Azima sources.

B. Anti-Azima Website Preservation

22. During my analysis, I directed the capture and preservation of the anti-Azima sources using the following methods.

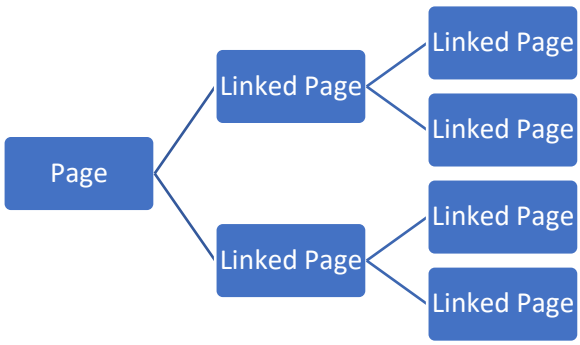
23. The pages were captured using Page Vault software, which documents the details of the capture (such as date and time; browser information; and capturing user, or "collector") and attaches a unique hash value to each capture for later authentication purposes.[9] Page Vault uses a remote browser, which prevents the collector from modifying any content on the page or its source code.[10]

24. For pages which required a user login to view, I used an examiner account (sometimes known as a "sockpuppet"). I did not interact with any other users of the sites, or request connection (or "friend") with any accounts.

25. I was initially provided with the URLs for two websites to capture: farhadazimascams[.]blogspot.com and exposedfarhadazima[.]wordpress.com. As part of my analysis, I discovered several other websites I believe were connected to the case and preserved them as well. For each URL, I captured the page with Page Vault, and reviewed its contents for links to additional pages. I then captured those linked pages and repeated the process of review and capture until all related pages were identified and captured.

[9] **See:** https://blog.page-vault.com/why-its-important-to-preserve-the-chain-of-custody-for-digital-evidence

[10] **See:** "How Legal Teams Use Self-Directed Software to Collect Admissible Online Evidence," Page Vault white paper published October 2023, https://blog.page-vault.com/how-legal-teams-use-self-directed-software-to-collect-admissible-online-evidence



26. I documented these pages in a spreadsheet, which tracked the URL, unique Page Vault Capture ID, and linked URLs for each, so the source of the captured URL could be identified in later analysis. I additionally documented the original and ultimate URLs for any redirected pages, and whether the page was currently online or defunct.

27. Because of incompatibility between Page Vault's browser and certain sites, I captured two of the 391 sites using a different software, Hunchly.[11] Hunchly is a software that Prescient uses in conjunction with a local web browser to capture pages as they are loaded passively, rather than at the specific direction of the collector.[12]

C. Investigation of Phishing Emails

28. I received 21 suspected phishing emails received by Azima and his associates between 2005 and 2016.

29. I was also provided with a December 2022 report authored by Meta titled "Threat Report on the Surveillance-for-Hire Industry" ("Meta Report"), which, among other details, includes an analysis of CyberRoot, which the Meta Report alleges is a surveillance-for-hire firm, i.e., a hacking firm.[13] The Meta Report concludes that CyberRoot uses tactics similar to those of another Indian surveillance-for-hire firm named BellTroX and that, according to public reporting,

[11] These were https://www.plurk[.]com/FarhadAzima and https://www.reddit[.]com/r/memes/comments/cz4gw0/farhad_azima_and_khater_massaad_latest_news/

[12] **See:** https://support.hunch.ly/category/50-hunchly-evidence-guide

[13] **See:** https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

CyberRoot and BellTroX have a history of working together and have shared the same web infrastructure and employees.[14] [15] The report also includes a list of indicators of compromise—phishing links and domains—associated with CyberRoot that were used to conduct their phishing campaigns. I investigated whether the phishing emails received by Azima and his associates contained the same tactics and infrastructure used by CyberRoot as detailed in the Meta Report.

30. Following receipt of this information, I analyzed the forensic data[16] contained in the suspected phishing emails received by Azima and his associates. I identified at least 15 links contained in the emails that indicate they were designed to conduct phishing attacks. The formats of the email messages and corresponding references to social media domains outside of the domain portion of the link, (e.g. "youtube.com" featured in link of xxxx.com/youtube.com), suggest to me that the links redirected to websites made to look like the login pages for various social media and other online platforms. Such sites are often designed to steal victims' login credentials and/or can also be used to infect their devices with malware.

31. For example, a May 19, 2015 email sent to Azima's email address "fa@fa1.us" was designed to look like a LinkedIn notification indicating Azima had received a message from another user. In that email message, I identified a link (in the "View Message" button, shown in the screenshot of the email, below) that contained the following URL:

> http://www.2ntigv4chn2hbk.mesvr[.]com/tg/2ntigv4chn2hblhttp/accounts-linkedin-com-servicelogin-addsession-v-en-us.look-com.org/-continue-https-maiil.gooogle.com-maiil.u.1.serviice-maiil.rpsnv.11-ct-1347523076345434376 4-rver.post/?to=&adroid=//accounts-linkedin-com-servicelogin-addsession-v-en-us.look-com.org/-continue-https-maiil.gooogle.com-maiil.u.1.serviice-maiil.rpsnv.11-ct-1347523076345434376 4-rver.post/m/?to=&msg=&red=//linkedin[.]com

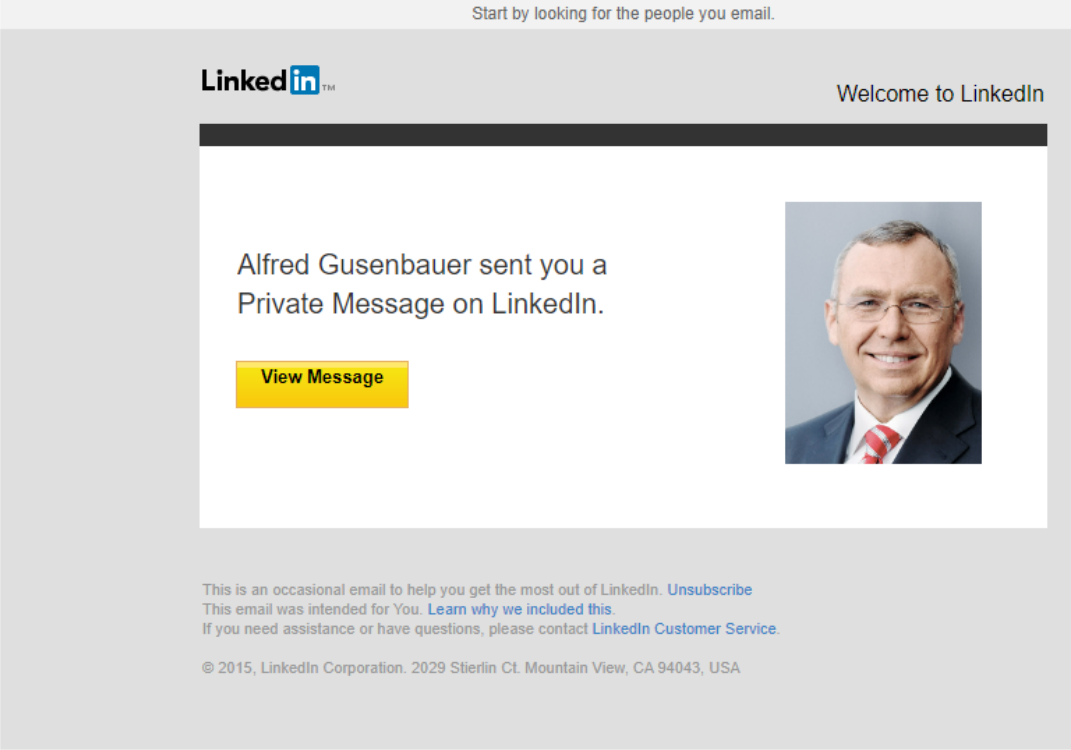
[14] **See:** https://www.reuters.com/article/cyber-lawsuit-belltrox/lawsuit-accuses-indian-hackers-of-leaking-businessmans-emails-idUSKBN2742EN/

[15] **See:** https://www.bloomberg.com/news/articles/2020-10-19/u-s-businessman-says-hacker-for-hire-firms-stole-his-data

[16] Forensic data is defined here and used in this report to refer to forensic objects that may or may not have some forensic value to an investigation. Among other elements, forensic data can include IP addresses, URLs, timestamps, logs, and files.

32. The link redirects victims to the domain look-com[.]org (highlighted in the above URL), among other domains. I note that the initial domain of "mesvr[.]com" is an online service designed to let users know when an email has been read.

From: "<Linkedin>" <messages-N0reply-linkedin@tech-center.com>
Sent: 5/19/2015 12:39:47 PM +0200
To: fa@fa1.us
Subject: Alfred Gusenbauer sent you a Private Message on LinkedIn.



33. I investigated look-com[.]org and the other domains contained in the links in the phishing emails. That investigation led me to discover various identifiers and other information relating to the domains including, but not limited to, domain registration records and associated IP addresses.

34. During this process, I identified dozens of IP addresses, domain registration records, and other identifying information associated with the domains. I then used those identifiers to further investigate the network infrastructure and any identifiable individuals or

organizations associated with the domains. I conducted searches on the surface, Deep, and Dark Web, a proprietary database of over 45 billion breached credentials, as well as open source and commercial investigative tools for investigating domains and associated network infrastructure.

35. My investigation of the identifiers associated with the phishing emails led me to locate a report and data published by the Citizen Lab[17] titled "Dark Basin: Uncovering a Massive Hack-For-Hire Operation" that focuses on Dark Basin, a hack-for-hire group that the Citizen Lab links to BellTroX with "high confidence."[18] The report includes a link to a folder on developer platform GitHub that contains a list of indicators of compromise ("IOCs") associated with Dark Basin including, among other indicators, domains and domain registrant email addresses tied to the group's hacking activities and network infrastructure they use(d). I utilized this data to investigate potential connections between the phishing emails and Dark Basin, BellTroX, and CyberRoot.

V. ANALYSIS: ANTI-AZIMA SOURCES

A. At Least 84 Sites/Pages Containing Links to Azima's Hacked Data or Anti-Azima Posts were Created from 2016 to Present, of which 26 were Created from October 2017 to Present

36. I identified a large number of anti-Azima sources that have been created since 2016. To date, I have identified 84 websites, blogs, social media platforms,[19] and other content-forward platforms that hosted anti-Azima information. Those 84 sites are:

- 1337x.to
- about.me
- adfty.biz
- angelfire.com
- artwanted.com
- bagtheweb.com

[17] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada, that conducts research on information and communication technologies, human rights, and global security. It is considered a credible source when it comes to spyware research.

[18] **See:** https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf

[19] In some cases, Prescient identified several social media accounts on a given social media platform hosting anti-Azima information.

- bebee.com
- behance.net
- bepress.com
- bibsonomy.org
- blogspot.com
- bookmark4you.com
- booksie.com
- bravesites.com
- briefingwire.com
- btcache.me
- commaful.com
- diigo.com
- discussion.community
- dribbble.com
- e27.co
- flipboard.com
- folkd.com
- freeprnow.com
- goodreads.com
- gravatar.com
- gust.com
- headshotcrew.com
- hubski.com
- imgflip.com
- imgur.com
- innovatorsedge.io
- livejournal.com
- medium.com
- memonic.com
- mendeley.com
- metatorrents.net
- mindmeister.com
- monova.org
- myfolio.com
- mystrikingly.com
- over-blog.com
- own-free-website.com
- pastebin.com
- pearltrees.com
- pinterest.com
- plurk.com
- poemhunter.com
- posteezy.com
- proboards.com
- professionalontheweb.com
- reddit.com
- remote.com
- schoolofeverything.com
- scoophot.com
- seedpeer.eu
- seekingalpha.com
- skyrock.com
- slashdot.org
- snapzu.com
- sociopost.com
- soup.io
- sparkpeople.com
- speakerdeck.com
- stage32.com
- steepster.com
- storybird.com
- sumotorrent.sx
- symbaloo.com
- the-dots.com
- thepiratebay.org
- triberr.com
- ttlink.com
- uniquethis.com
- voat.co
- wattpad.com
- wellfound.com
- wetransfer.com
- wordpress.com (5)
- zumvu.com

37. I identified data on 44 of these anti-Azima sources which indicate the sites were created or began hosting anti-Azima content between August 2016 and January 2020, broken down as follows:

- 2016 – 16 anti-Azima sources[20]
- 2017 – One anti-Azima source
- 2018 – 11 anti-Azima sources
- 2019 – 13 anti-Azima sources
- 2020 – Two anti-Azima sources

38. I was able to determine that 26 of these anti-Azima sources were created or began hosting anti-Azima information after October 2017 and that, as described below, these sources appear to be part of a coordinated campaign targeting Azima.

39. The abovementioned anti-Azima sources can be divided into the following categories.[21]

40. **Torrent Sites:** Prescient identified seven torrent sites. As of January 2024, two of these torrent sites contain links to torrent files which appears to contain metadata that would have allowed a user to download Azima's data (it was not possible to download the data because the torrents did not have any active seeders,[22] but the meta-data of the torrent files indicate they contain Azima's data). Five of the torrent sites are currently offline, but based on their titles and/or context, appear to have at some point provided users with the ability to download at least some of Azima's data. The seven torrent sites are:

- thepiratebay[.]org/torrent/15484452 - **active**
- 1337x[.]to/user/anjames/ - **active**[23]
- btcache[.]me/torrent/5d65707106c1c7a0562d16f6ae6c90b1aa594b18 - **defunct**

[20] On some of the identified anti-Azima sources, activity (such as additional posts, updates, or other forms of activity) was detected after this date. This year of demarcation is specifically the date that the anti-Azima source was created or first logged activity, but does not necessarily indicate that further activity was not detected in subsequent years.

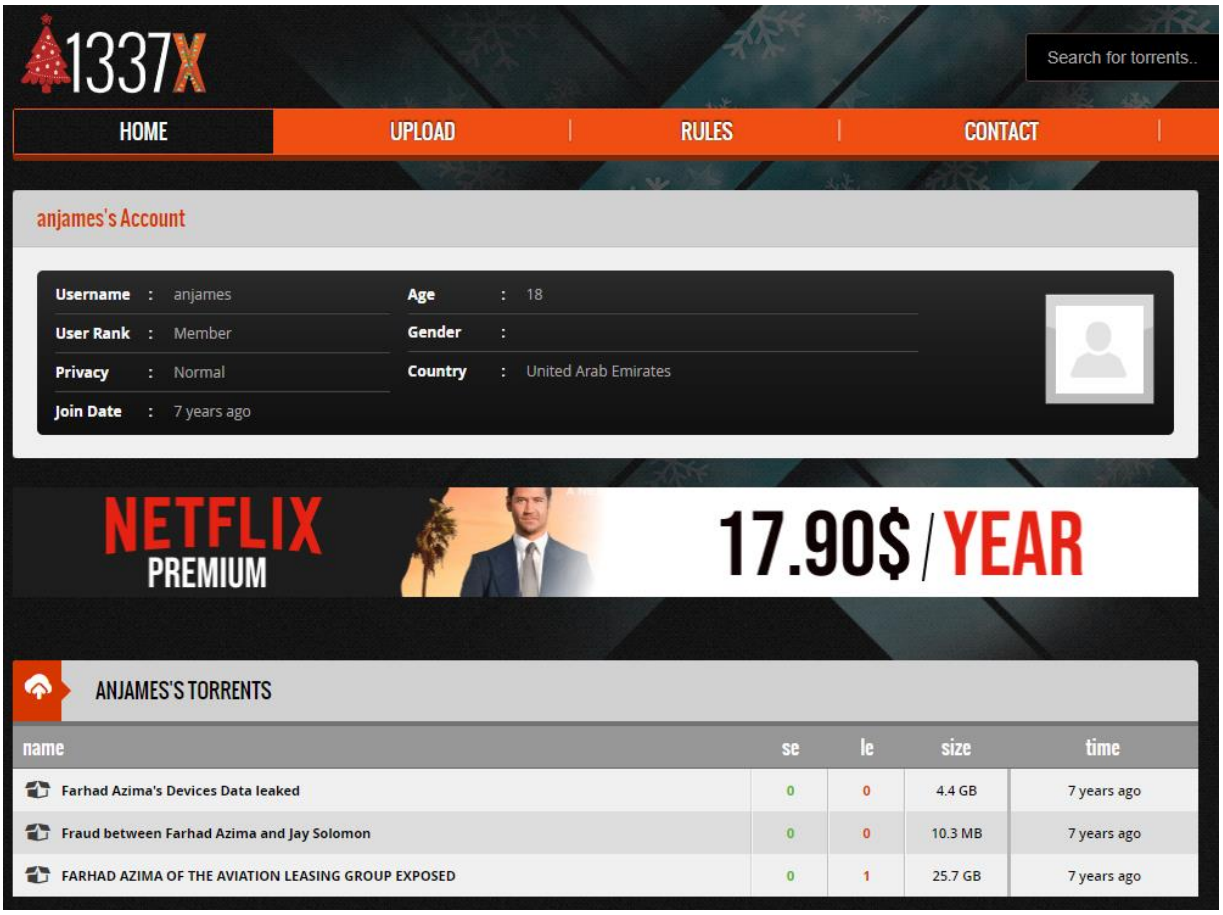
[21] Categories are not mutually exclusive, as some sites identified cover multiple categories.

[22] Seeders are torrent site users who are sharing a file(s) with other users.

[23] This webpage for the user "anjames" provides links to three torrents.

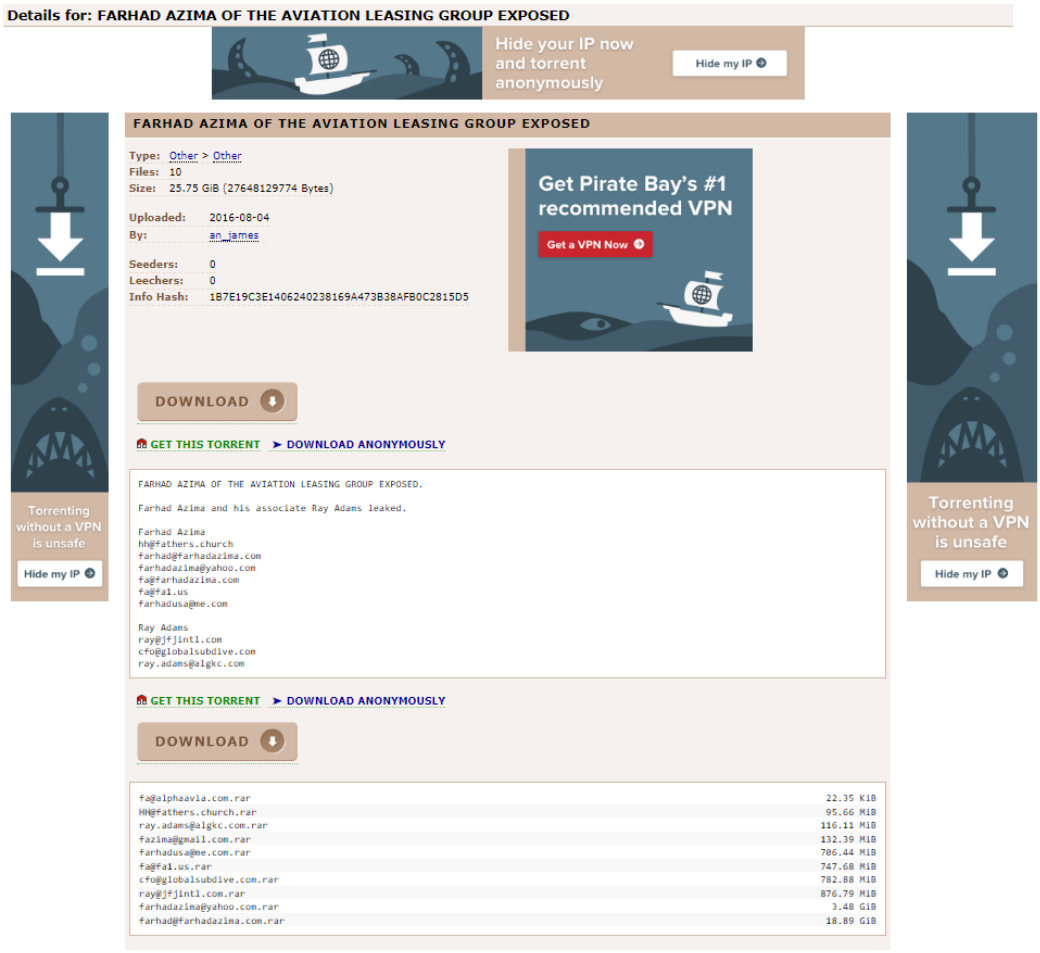
- metatorrents[.]net/torrent/15484452/farhad+azima+of+the+aviation+leasing+group+exposed - **defunct**
- sumotorrent[.]sx/en/details_10762203.html - **defunct**
- seedpeer[.]eu/details/11694381/farhad-azima's-devices-data-leaked.html - **defunct**
- monova[.]org/42248895 - **defunct**

41. Prescient identified file upload date information on the two active torrent sites. Approximately seven years ago, an account under the username "anjames" with a reported location of United Arab Emirates and a listed age of 18 uploaded three torrent files containing what appears to be Azima's data to torrent website 1337x.[24]



[24] **See:** https://1337x[.]to/user/anjames/

42. In addition, on August 4, 2016 an account under the username "an_james" uploaded a torrent file containing what appears to be Azima's data to torrent website thepiratebay.org.[25]



43. **Websites Containing Links to Azima's Data on WeTransfer:** I identified three websites that host links to files on file sharing website WeTransfer that at one point purportedly contained data taken from devices maintained by Azima. Those three websites are: farhadazimascandal.page[.]tl, exposedfarhadazima.wordpress[.]com, farhadazimascams.blogspot[.]com.

44. On an unknown date, an anonymous user posted links to file sharing website

[25] **See:** https://thepiratebay[.]org/torrent/15484452

WeTransfer (hyperlinked via "Download" text prompt in screenshot, below) on website farhadazimascandal.page[.]tl.[26] The webpage also included a link that directed users to the torrent files on thepiratebay[.]org described above.

farhad azima

FARHAD AZIMA

Farhad Azima is such a big scammer. Some reports claim that he found guilty in US major scams though Azima has always claimed that he know nothing.

Find some links to read more about Farhad Azima scandal:

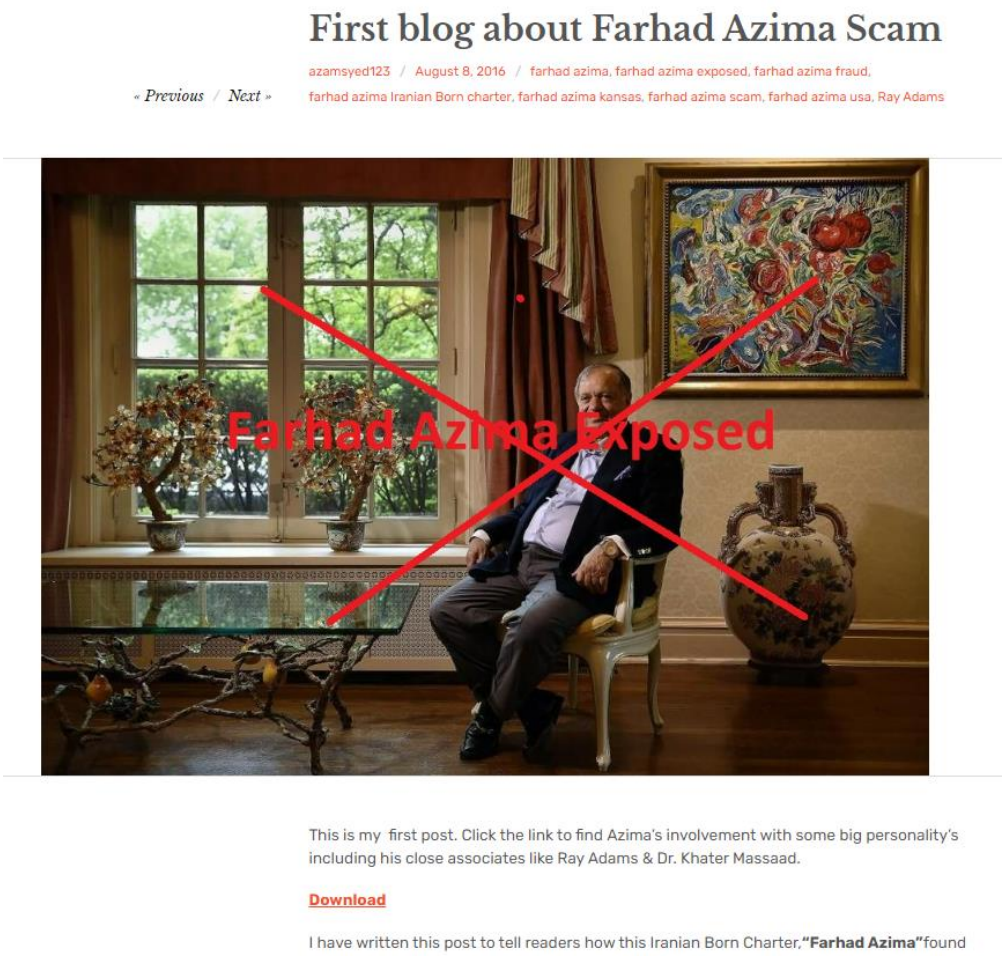
https://thepiratebay.org/torrent/15484452

Download

45. On an unknown date between August 8, 2016 and June 9, 2019 an account under the username "azamsyed123" posted a link to the file sharing website WeTransfer on exposedfarhadazima.wordpress[.]com.[27] These links were hyperlinked in a "Download" text prompt as show in the screenshot below. During approximately the same time period, the creator of the website also posted links to files that purportedly contained Azima's data hosted on various torrent websites.

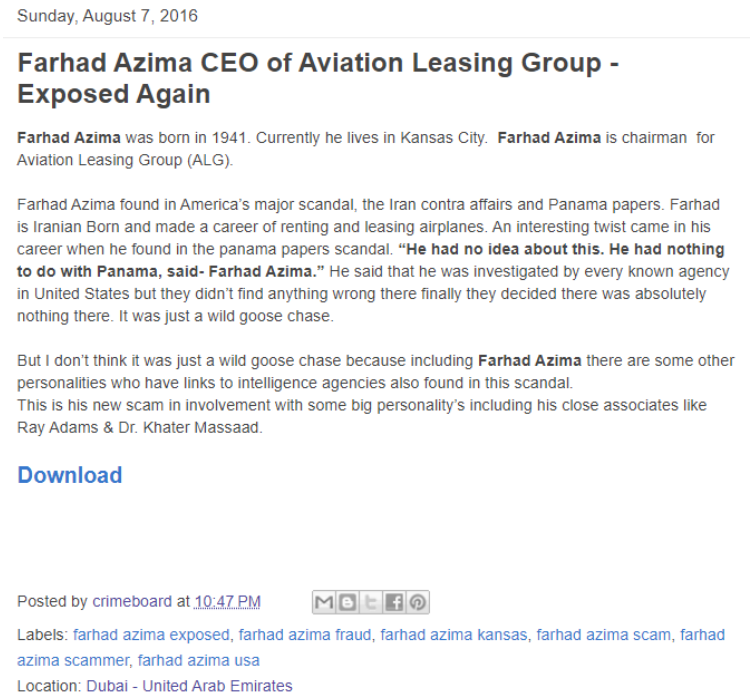
[26] **See:** http://farhadazimascandal[.]page.tl/

[27] **See:** https://exposedfarhadazima.wordpress[.]com/2016/08/08/farhad-azima-farhad-azima-scammer/



46. On an unknown date between August 7, 2016 and June 6, 2019 an account under the username "crimeboard" posted a link to the file sharing website WeTransfer on blog site farhadazimascams.blogspot[.]com.[28] This link was hyperlinked in a "Download" text prompt as show in the screenshot below. The post containing the link says that the post was made from Dubai, United Arab Emirates, with the GPS coordinates 25°12'17.5"N 55°16'14.8"E.[29] During approximately the same time period, the creator of the website also posted links to files that purportedly contained Azima's data hosted on various torrent websites.

[28] **See:** https://farhadazimascams.blogspot[.]com/2016/08/farhad-azima-ceo-of-aviation-leasing.html
[29] Which geolocate to the general location of Al Safa Street, Dubai, United Arab Emirates.



Sunday, August 7, 2016

Farhad Azima CEO of Aviation Leasing Group - Exposed Again

Farhad Azima was born in 1941. Currently he lives in Kansas City. **Farhad Azima** is chairman for Aviation Leasing Group (ALG).

Farhad Azima found in America's major scandal, the Iran contra affairs and Panama papers. Farhad is Iranian Born and made a career of renting and leasing airplanes. An interesting twist came in his career when he found in the panama papers scandal. **"He had no idea about this. He had nothing to do with Panama, said- Farhad Azima."** He said that he was investigated by every known agency in United States but they didn't find anything wrong there finally they decided there was absolutely nothing there. It was just a wild goose chase.

But I don't think it was just a wild goose chase because including **Farhad Azima** there are some other personalities who have links to intelligence agencies also found in this scandal.
This is his new scam in involvement with some big personality's including his close associates like Ray Adams & Dr. Khater Massaad.

Download

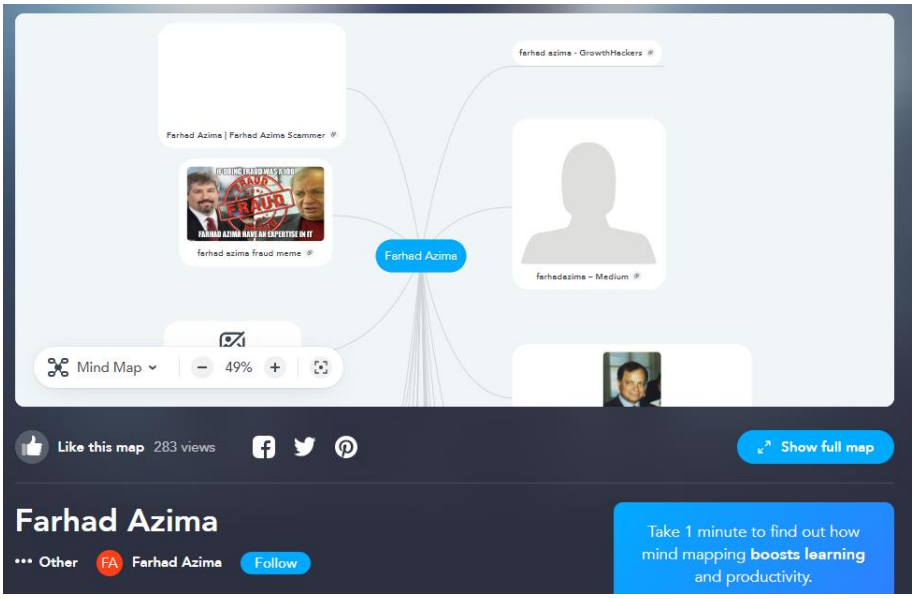
Posted by crimeboard at 10:47 PM

Labels: farhad azima exposed, farhad azima fraud, farhad azima kansas, farhad azima scam, farhad azima scammer, farhad azima usa
Location: Dubai - United Arab Emirates

47. **Websites and Social Media Platforms that Include Links to Websites with Links to Torrents or WeTransfer:** I identified at least 38 websites and social media platforms that include links to the abovementioned sites that contained links to torrent sites or WeTransfer as described above. These anti-Azima sources were created or contain posts that were published between August 2016 and January 2020.

48. The most recent site that I found was on the mind mapping social media platform MindMeister. [30] According to data obtained from the platform via a subpoena request, on an unknown date between January 2, 2020 and January 16, 2020 an account under the name "Farhad Azima" created a mind map with links to exposedfarhadazima.wordpress[.]com and other sites with anti-Azima information.

[30] **See:** https://www.mindmeister[.]com/1392200781/farhad-azima



49. **Websites and Social Media Accounts Critical of Azima's Business Practices:** In addition to the abovementioned anti-Azima sources, I identified several other websites and social media accounts that contain content critical of Azima's business practices. These anti-Azima sources were created or published posts between August 2016 and January 2020. Most of these anti-Azima sources include content accusing Azima of being part of a fraudulent scheme. For example, a December 16, 2019 post titled "SOME BIGGEST FRAUDS AND THEIR DOER" was published by an unknown actor on blog farhadazima.over-blog[.]com, a blog site created with a URL that includes Azima's name.[31] Among other accusations, the blog post accuses Azima and several other individuals of being "scammers" and "conmen."

[31] **See:** http://farhadazima.over-blog[.]com/2019/12/some-biggest-frauds-and-their-doer.html

JHO LOW, RANDY GLASS, WILL Z. MCFARLAND, YVONNE BANNIGAN, FARHAD AZIMA, KHATER MASSAAD, A HOLLYWOOD EXECUTIVE IMPERSONATOR

SOME BIGGEST FRAUDS AND THEIR DOER

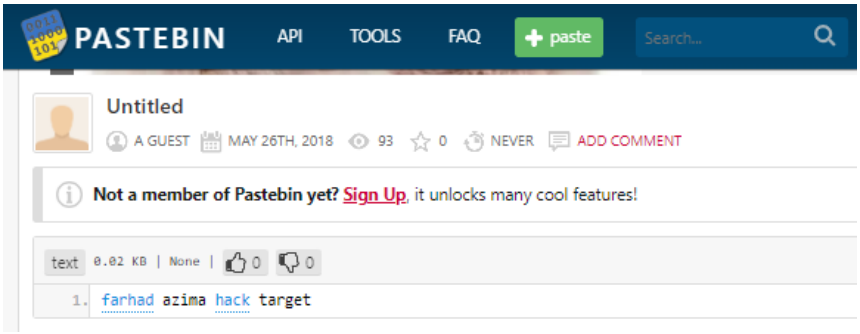
DECEMBER 16 2019

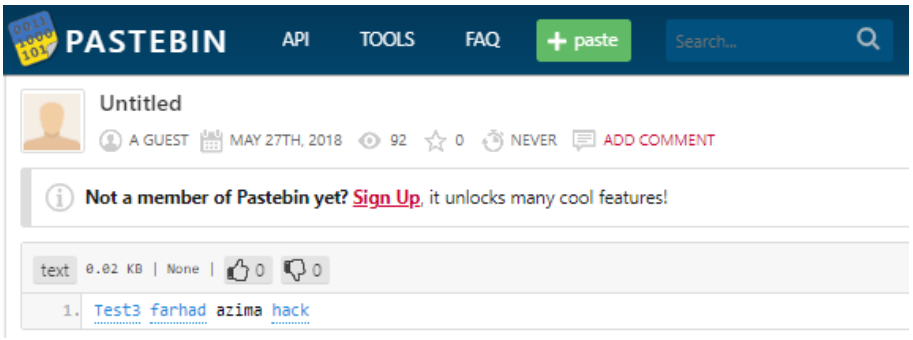
In this article, I am going to highlight some biggest fraud which I have read till now. And would like to share with people how they can take get experience from these real-life fraudsters. I am sure it provides some insight to people who are already on hard time and can face some near situation in their near future because scammers take advantage of those innocent people. The inside reality is, there are always people (scammer/fraudster) out there who looking for people (victims) they can easily get advantage of them. You can also find number of scammers/conmen on cyber space. Farhad Azima, Jay Solomon, Dr. Khater Massaad, Ray Adams, Jho Low, Randy Glass, Will Z. McFarland, Yvonne Bannigan, A Hollywood executive impersonator are few of them.

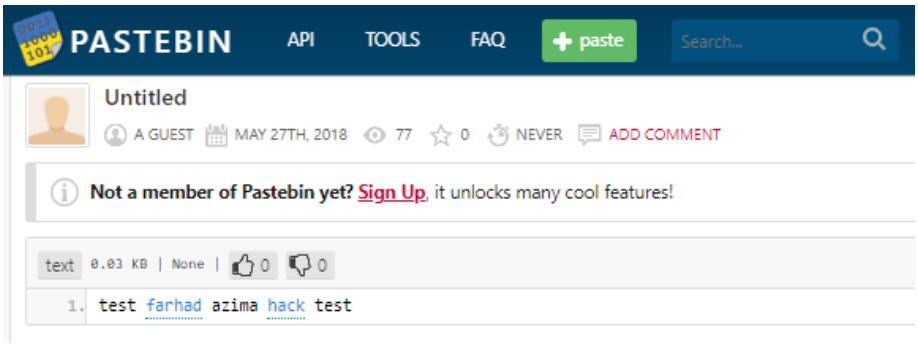
50. **Paste Sites with References to Azima and Hacking:** I identified eight posts on paste site Pastebin published between May 26, 2018 and June 1, 2018 that reference Azima and hacking, with several appearing to refer to him as a "target."[32] [33] [34] [35] [36] [37] [38] [39] Paste sites are sites that allow users to store and share text-based information. Paste sites typically provide users with a simple interface to paste their content, which is then saved as a unique URL that can be shared with others. Paste sites are often used by cybercriminals to share information anonymously. Owing

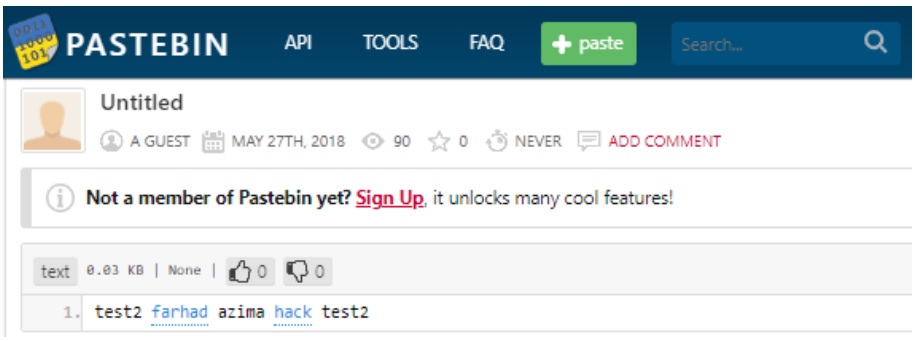
[32] **See:** https://pastebin[.]com/EZ8MpsZG
[33] **See:** https://pastebin[.]com/YkEFCnv0
[34] **See:** https://pastebin[.]com/34q1W1mn
[35] **See:** https://pastebin[.]com/f0S6Nd61
[36] **See:** https://pastebin[.]com/ns7buKZY
[37] **See:** https://pastebin[.]com/Ne8MK66e
[38] **See:** https://pastebin[.]com/e7fnzK2r
[39] **See:** https://pastebin[.]com/pPxy3N58

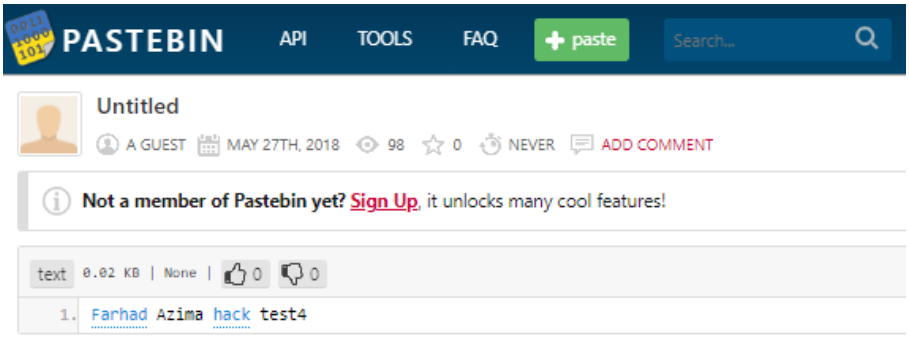
to a lack of contextual information relating to these posts, I was unable to determine their purpose or intent. Screenshots of these sites are included below:

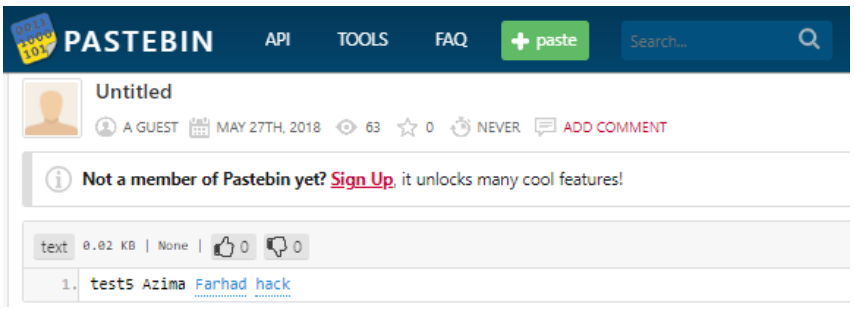


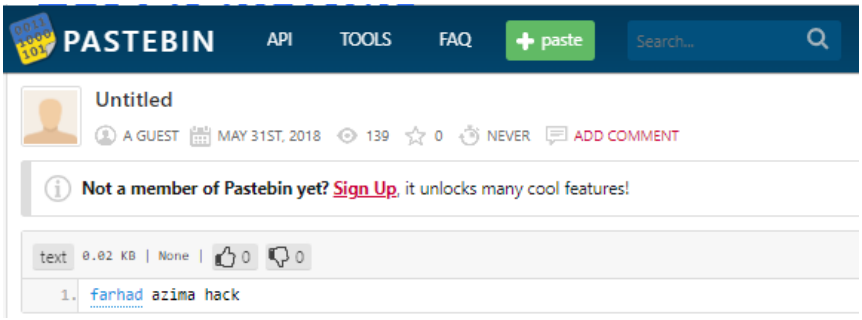


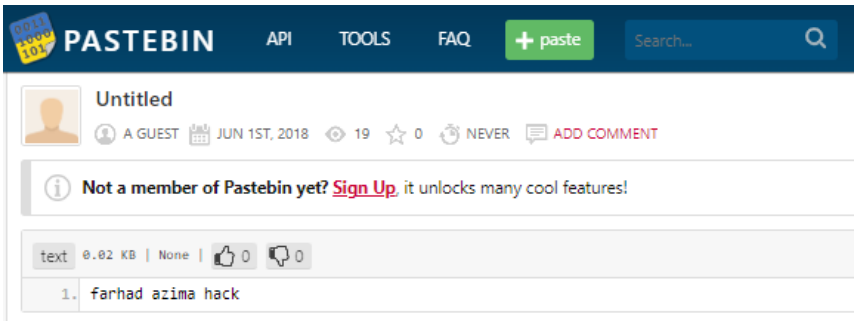










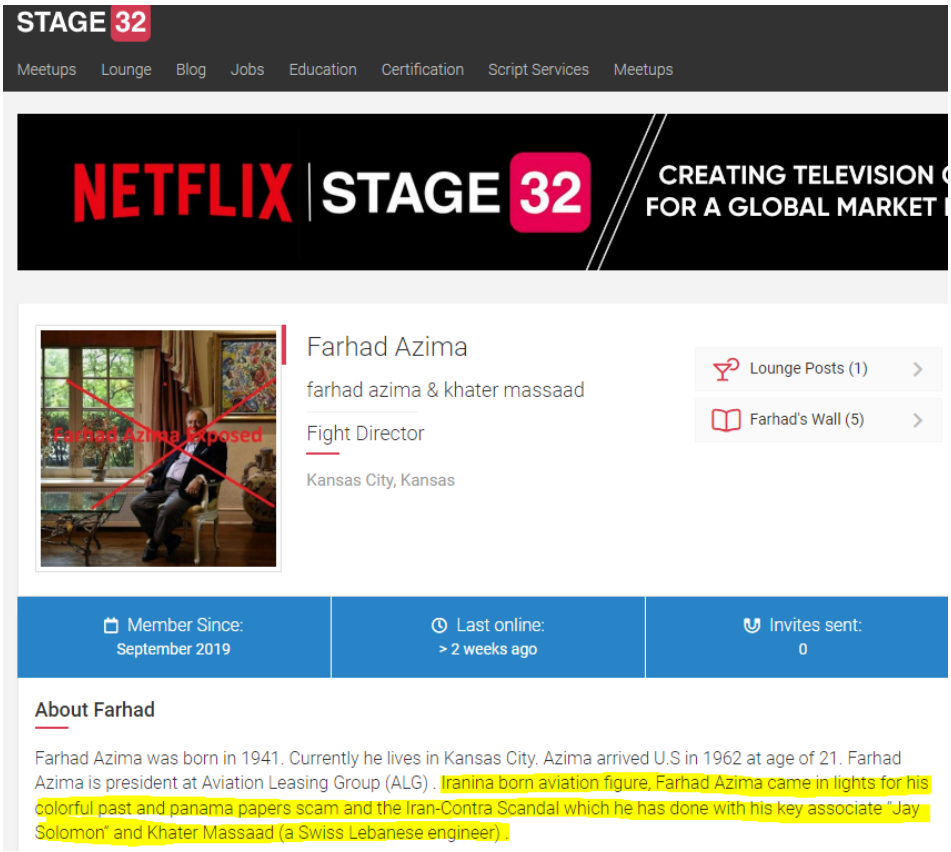


B. The Anti-Azima Sites Share Common Indicators Suggesting They Are Part of a Coordinated Campaign

51. It is my opinion that the abovementioned anti-Azima sources appear to be connected and are part of a coordinated campaign targeting Azima perpetrated by the same person

or group of people. My reasoning for this opinion is detailed below.

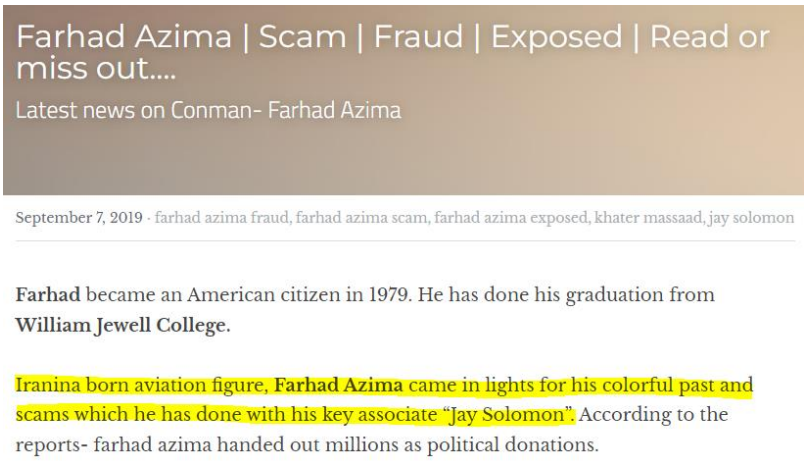
52. **Similar Language Use and Style of Writing:** Many of the anti-Azima sites that I found feature similar, if not the exact same language and style of writing, including the exact same typo. For example, I identified an account created in September 2019 under the name "Farhad Azima" on social media platform Stage 32 that has an "About" section that includes the following sentence, "Iranina [sic] born aviation figure, Farhad Azima came in lights for his colorful past and panama papers scam and the Iran-Contra Scandal which he has done with his key associate 'Jay Solomon' and Khater Massaad (a Swiss Lebanese engineer) ."[40]



53. The near exact same language was identified in a September 7, 2019 post identified on blog site farhadazimasite.mystrikingly[.]com that includes the wording, "Iranina [sic] born

[40] **See:** https://www.stage32[.]com/farhadazima

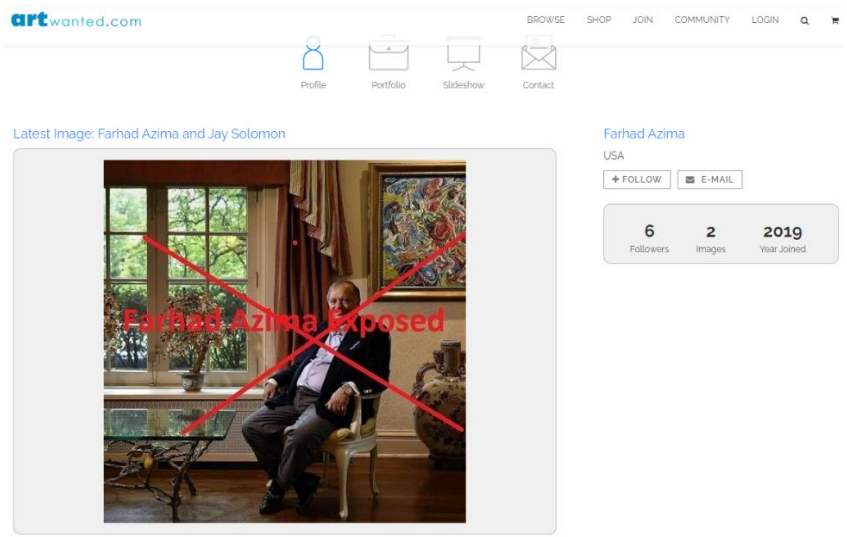
aviation figure, Farhad Azima came in lights for his colorful past and scams which he has done with his key associate 'Jay Solomon'."[41]

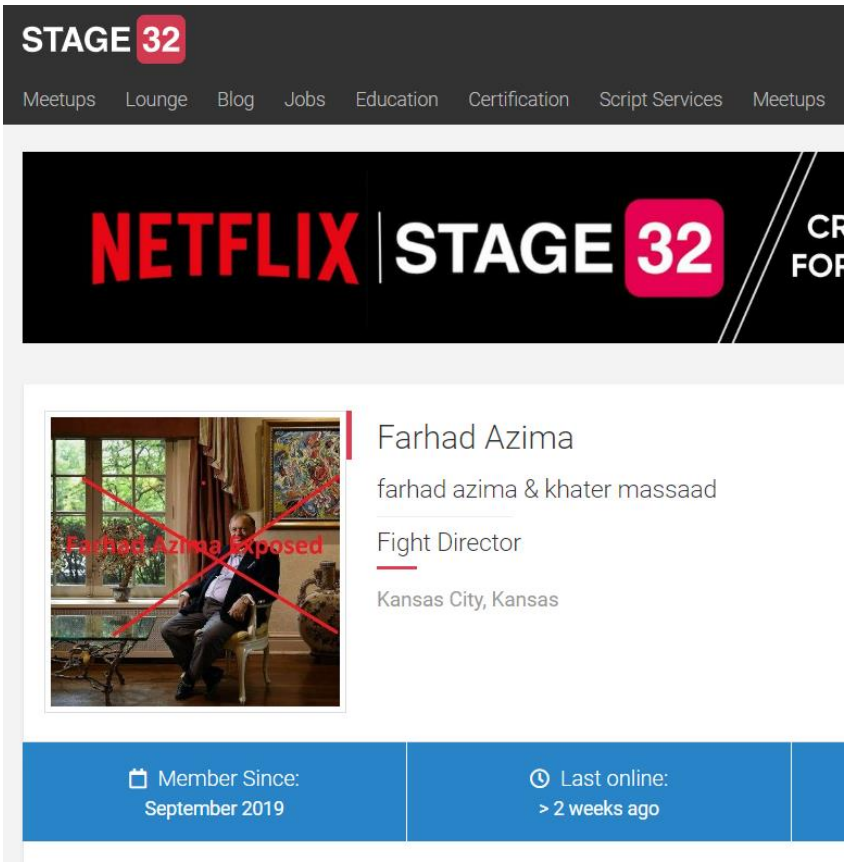


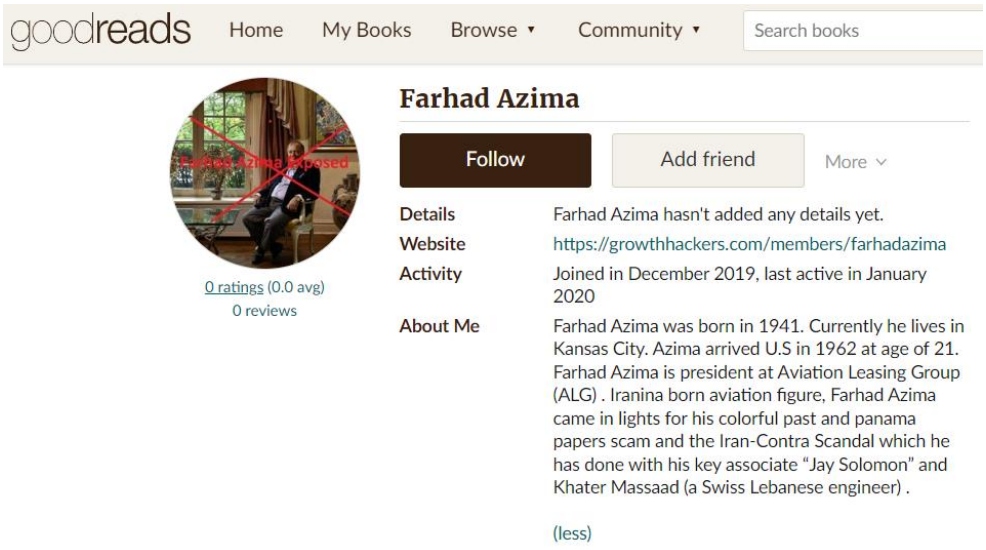
54. Both sites include the identical misspelling of Iranian ("Iranina") and usage of quotation marks around the name "Jay Solomon." Both also use the distinctive phrase "came in lights for his colorful past." I am of the opinion that it is very unlikely that these similarities of language use and writing are random, and it is more likely that these posts were created by the same individual(s) as part of a coordinated effort to smear Azima.

55. **Duplication of Images:** Dozens of the anti-Azima sites that I found include the same images featuring Azima. In particular, I observed the repeated use of an image of Azima with red lines in the shape of an "X" and red text that read "Farhad Azima Exposed." A representative sample of anti-Azima sources that include the duplicative use of such images is shown below.[42] [43] [44]

[41] **See:** https://farhadazimasite.mystrikingly[.]com/blog/farhad-azima-scam-fraud-exposed-read-or-miss-out
[42] **See:** https://www.artwanted[.]com/farhadazima
[43] **See:** https://www.stage32[.]com/farhadazima
[44] **See:** https://www.goodreads[.]com/user/show/106321378-farhad-azima


artwanted.com
BROWSE
SHOP
JOIN
COMMUNITY
LOGIN
Profile
Portfolio
Slideshow
Contact
Latest Image: Farhad Azima and Jay Solomon
Farhad Azima Exposed
Farhad Azima
USA
+ FOLLOW
E-MAIL
6
Followers
2
Images
2019
Year Joined


STAGE 32
Meetups
Lounge
Blog
Jobs
Education
Certification
Script Services
Meetups
NETFLIX | STAGE 32
Farhad Azima Exposed
Farhad Azima
farhad azima & khater massaad
Fight Director
Kansas City, Kansas
Member Since:
September 2019
Last online:
> 2 weeks ago



56. I also observed the repeated use of an image of Azima and another individual with the words "FRAUD" and "IF DOING FRAUD WAS A JOB FARHAD AZIMA HAVE AN EXPERTISE IN IT."[45] [46]

[45] **See:** https://imgflip[.]com/i/39k6qa
[46] **See:** https://farhadazimasite.mystrikingly[.]com/

imgflip Create

farhad azima fraud meme

ALL THE PARTS YOU NEED FOR YOUR TRAILERS
THE TRAILER PARTS OUTLET
Shop Now

share

2,679 views · 30 upvotes · Made by farhadazima 4 years ago in fun

farhadazima khatermassaad funny memes imgflip voter fraud

INK BLOG

ABOUT BLOG CONNECT

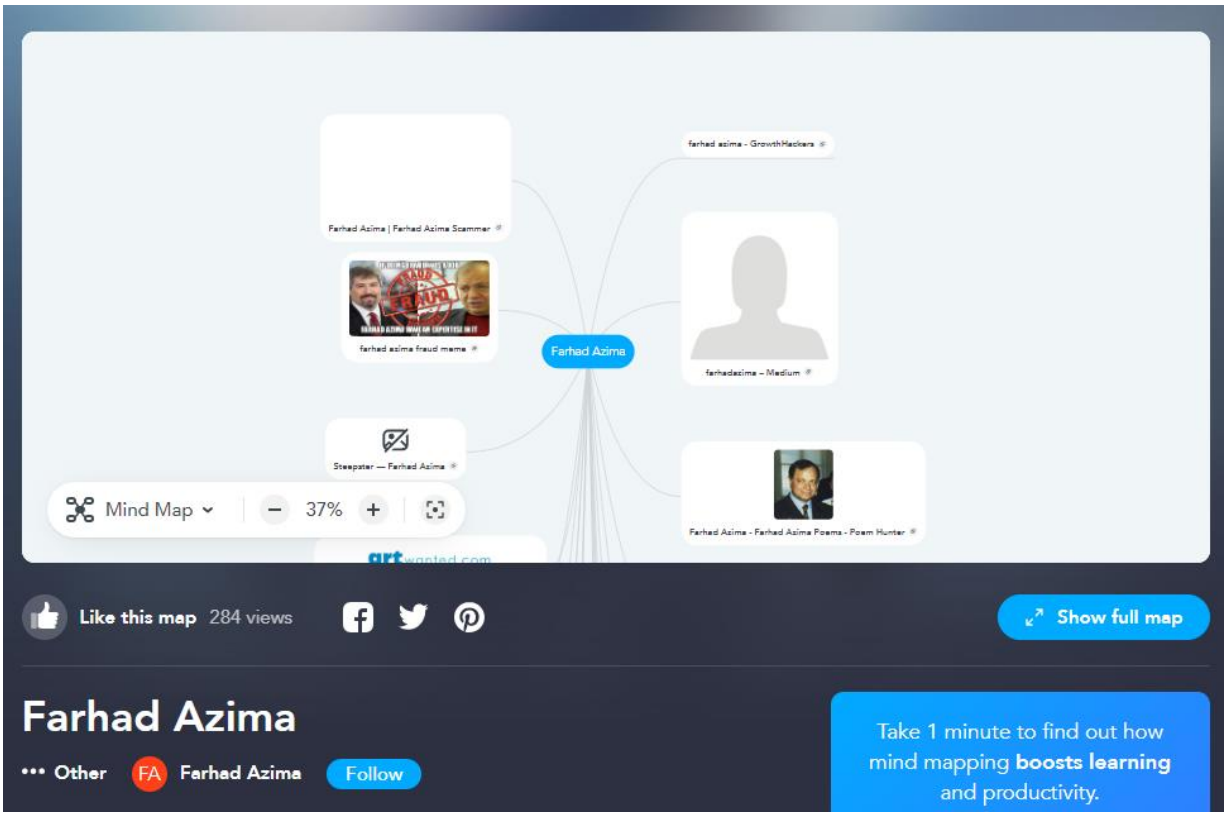
Farhad Azima & Jay Solomon Fraud

Farhad Azima was born in 1941. Currently he lives in Kansas City.
Farhad Azima is chairman for Aviation Leasing Group (ALG).
Farhad Azima found in America's major scandal

FOLLOW FOR MORE NEWS ON FARHAD!

57. The use of the same images by individuals across several platforms is a strong indicator to me that these anti-Azima sources were created by the same individual(s).

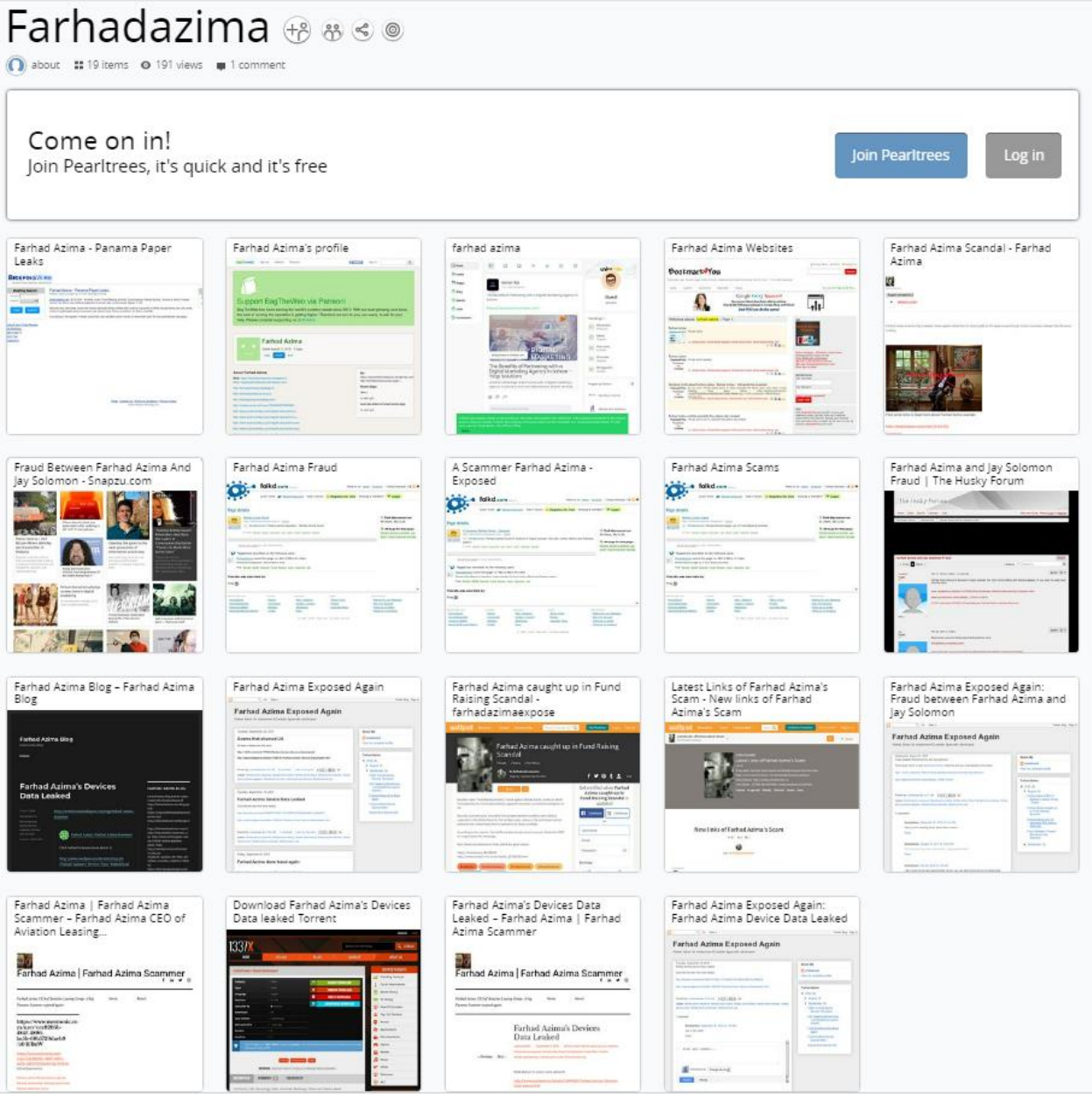
58. **Bookmarking and Social Media Accounts Collating and Sharing Links to Identical or Similar Anti-Azima Sources:** I identified several accounts on bookmarking and social media platforms that have collected and posted links to dozens of the abovementioned anti-Azima sources. For example, as described above, I identified a January 2020 mind map posted on Mindmeister by an account under the name "Farhad Azima" that includes over a dozen links to anti-Azima sources.[47]



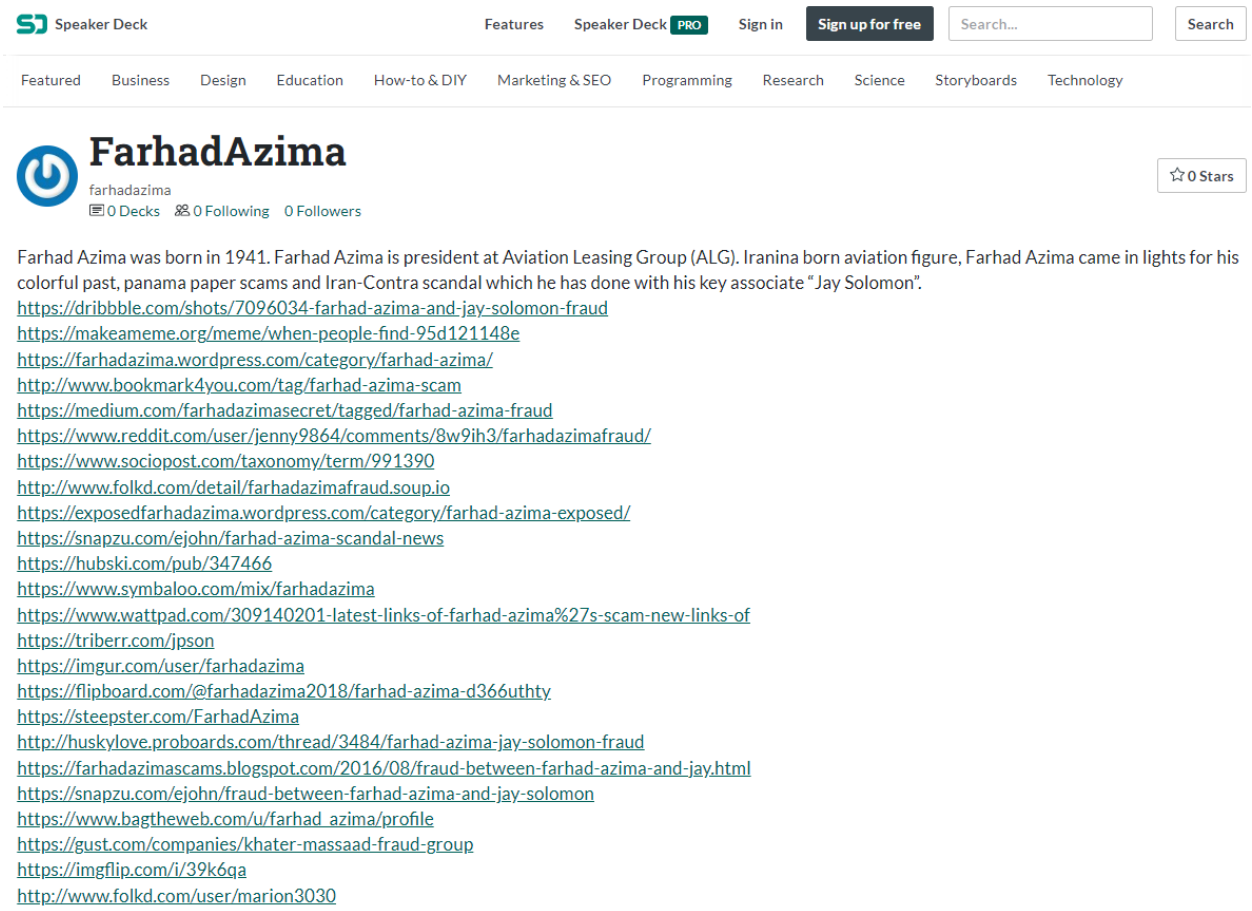
59. A representative sample of other accounts I found on bookmarking and social

[47] **See:** https://www.mindmeister[.]com/1392200781/farhad-azima

media platforms that also include links to dozens of anti-Azima sources is shown below.[48] [49]



[48] **See:** http://www.pearltrees[.]com/farhadazima
[49] **See:** https://speakerdeck[.]com/farhadazima



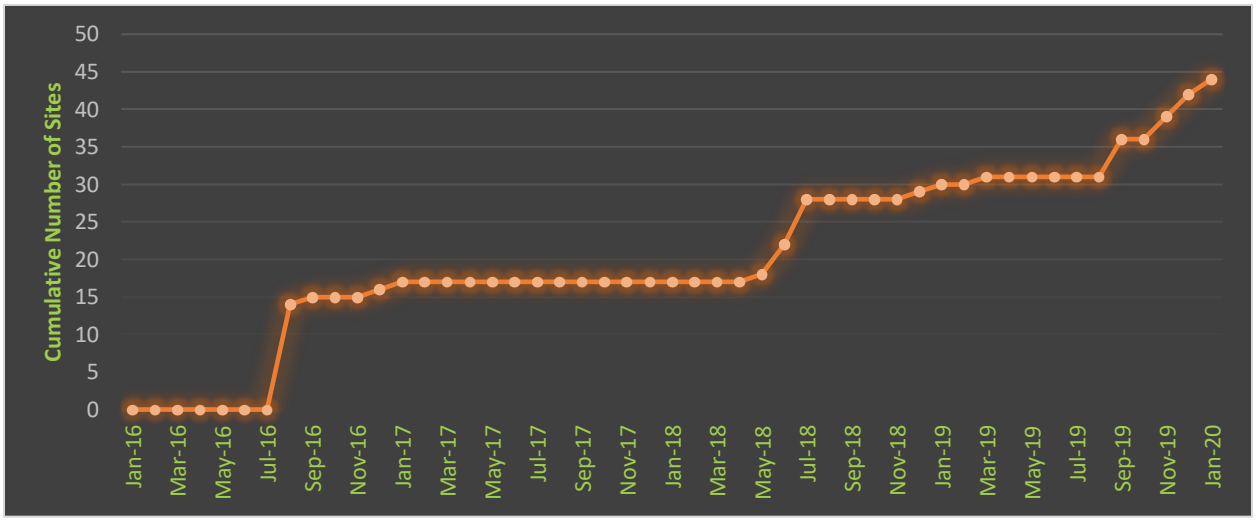
60. The collation and sharing of so many of these links by individual accounts on these platforms indicates to me that the creation of these anti-Azima sources was a concerted and coordinated effort by an individual or group of individuals.

61. The cross-linking nature of many of the anti-Azima sources is a further indication of this concerted effort because a common tactic to increase the page ranking on major search engines like Google is to increase the number of links to a website.

62. **Coordinated and Increased Posts Around Several Distinct Time Periods Timing:** Several anti-Azima sources were created during the same time periods, which I believe to be a sign of coordinated activity.

63. The chart below, also attached as Appendix B, shows the cumulative number of

anti-Azima sources created between 2016 and 2020.



64. I identified 14 anti-Azima sources that were created within the month of August 2016:

1. briefingwire[.]com/pr/farhad-azima-panama-paper-leaks
2. bookmark4you[.]com/user/2269909-aabid236
3. exposedfarhadazima.wordpress[.]com/
4. farhadazima.livejournal[.]com/
5. farhadazimascams.blogspot[.]com/
6. flipboard[.]com/@farhadazima2018
7. folkd[.]com/profile/FarhadAzima
8. freeprnow[.]com/pr/panama-paper-farhad-azima-scandal
9. hubski[.]com/user/k12
10. plurk[.]com/FarhadAzima
11. reddit[.]com/user/Aabid236
12. snapzu[.]com/ejohn
13. thepiratebay[.]org/torrent/15484452

14. wattpad[.]com/user/farhadazimaexpose

65. Ten anti-Azima sources were then created within the two-month period between June and July 2018:

1. azimaconmanfarhadazima.wordpress[.]com
2. azimathief.wordpress[.]com
3. diigo[.]com/profile/sahargulahsan
4. e27[.]co/user/farhadazima
5. https://azimafraud.wordpress[.]com
6. imgur[.]com/user/farhadazima
7. pastebin[.]com/xZA8jNRH
8. pearltrees[.]com/farhadazima
9. schoolofeverything[.]com/person/sahargulahsan
10. ttlink[.]com/pc

66. Additionally, seven anti-Azima sources were created during the three-month period between September and November 2019:

1. artwanted[.]com/farhadazima
2. commaful[.]com/play/farhadazima/
3. farhadazimasite[.]mystrikingly.com
4. pinterest[.]com/khaterfarhadazima
5. slashdot[.]org/~farhadazimascam
6. stage32[.]com/farhadazima
7. symbaloo[.]com/mix/farhadazima

67. In my opinion, surges of new content that reference a relatively esoteric topic during the same periods indicates some degree of coordination. That these sources feature many

similarities as discussed above further cements my opinion.

68. **Consistent use of Virtual Private Networks and Proxy IP Addresses:** I identified and analyzed the IP addresses associated with dozens of anti-Azima sources. Many of these IP addresses share similar characteristics in that many are associated with virtual private network ("VPN") and/or proxy services. VPNs and proxy services enable users to establish a digital connection between their computer and a remote server owned by a VPN or proxy service provider, creating a point-to-point tunnel or gateway that encrypts their personal data and masks their IP address. These services are often used by malicious online actors to obfuscate their IP addresses to prevent identification. The table below shows a summary of information associated with a representative sample of the IP addresses associated with anti-Azima sources.

IP Address	Associated Anti-Azima Source Information	IP Address Type	Provider	IP Address Location
194.36.111.59	Last recorded IP address associated with Mindmeister user "Farhad Azima" on January 16, 2020	VPN	M247	Secaucus, New Jersey, U.S.
213.152.162.5	IP address used by user "azamsyed123" to make June 6, 2019 post on exposedfarhadazima.wordpress[.]com	VPN	Global Layer B.V.	Haarlem, Netherlands
213.152.162.154	Captured IP address used by user "farhadazima" to create website farhadazima.wordpress[.]com on September 12, 2016	VPN	Global Layer B.V.	Haarlem, Netherlands
84.39.116.0	Captured IP address used by user (user ID: 588180709863) to modify post (ID: 588180709863) on blog site farhadazimascams.blogspot[.]com on May 24, 2018	VPN	M247	Salford, United Kingdom

69. While the use of VPNs and proxy IP addresses is certainly increasing, the fact that many of the sites were created using such services (where that information was available) indicates

to me that the individuals responsible have a certain degree of cyber sophistication. That individuals associated with the anti-Azima sources happened to choose the same VPN/proxy IP address providers on multiple occasions also indicates a certain degree of collaboration between individuals or that it was the same individual.

C. Conclusion

70. Based on my investigation, I am of the opinion that the identified anti-Azima sources were likely created by the same individual or group of individuals as part of a coordinated smear campaign targeting Azima that began as late as 2016 and continued until at least 2020. There was an increase over time from 16 posts/pages at the end of 2016 to 44 in early 2020, with 26 created from October 2017 forward. There were three time periods when there was a distinct increase in posting anti-Azima sources: August 2016; between June and July 2018; and between September and November 2019. When you factor in the similarities in language across the sources, the use of exact same or similar images, backlinks[50] between the sources (including certain sources that consisted only of backlinks to other sources); and consistent use of VPNs to post content it becomes increasingly likely that the anti-Azima sources are linked and are part of a coordinated campaign against Azima. The individual or group behind this activity sought to share Azima's data with public audiences and publish negative content critical of Azima's business practices in a sustained manner over several years.

VI. ANALYSIS: PHISHING EMAILS

A. Investigation of Phishing Emails Received by Azima Suggests Some Were Sent by CyberRoot and/or BellTroX.

71. As described above, I also analyzed 21 phishing emails received by Azima or his

[50] "backlinks" are links from one website to another

associates, and compared those phishing emails to techniques and sites associated with CyberRoot and BellTroX.

72. Through my analysis of the links contained in the 21 phishing emails I found several domains common to the linked URLs.

73. A non-exhaustive list of these domains are as follows:[51]

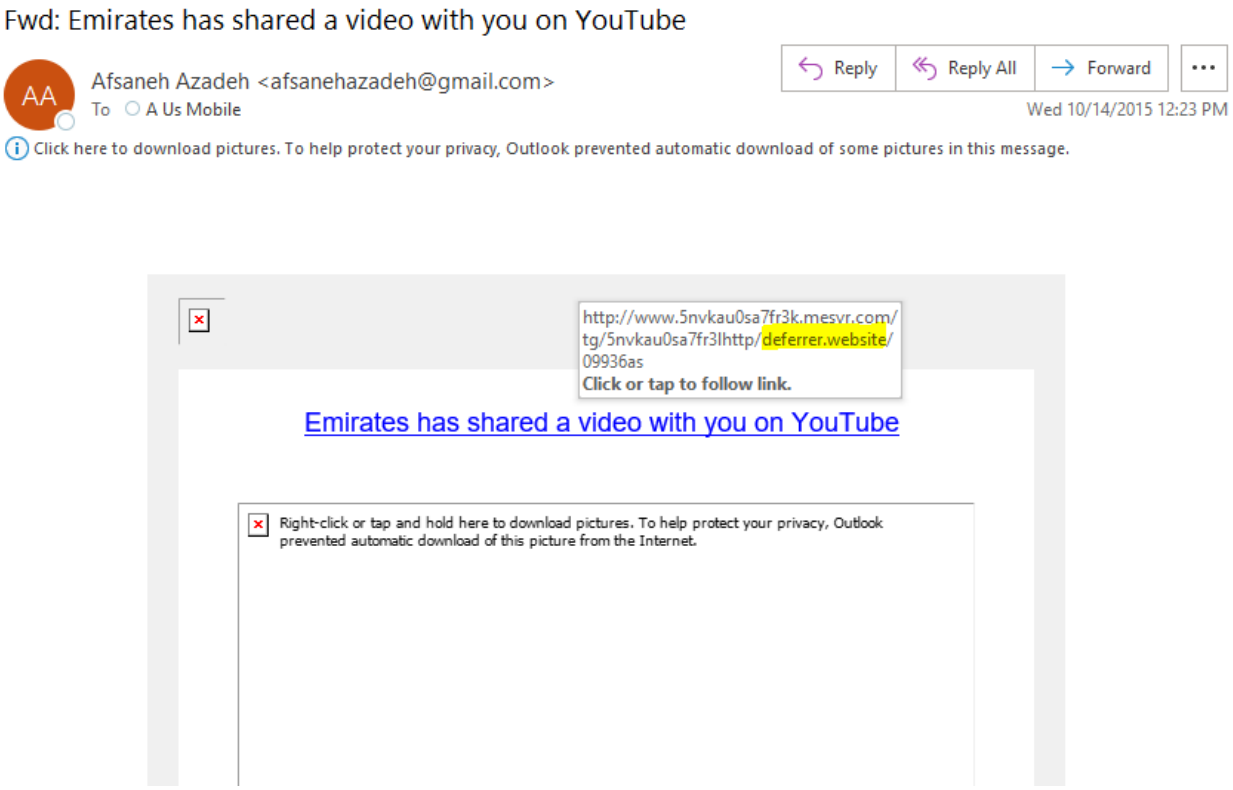
- look-com[.]org
- deferrer[.]website
- secureddownloadfolder[.]com
- secureredirect[.]link
- internetsecuritystandards[.]website
- mesvr[.]com

74. I investigated each of these domains and for two of the domains, deferrer[.]website and look-com[.]org, identified possible links to CyberRoot and/or BellTroX, as detailed below.

B. deferrer[.]website

75. Six of the phishing emails Mr. Azima or his associates received contain links to content hosted on the domain deferrer[.]website, which I have determined has possible links to CyberRoot and/or BellTroX. For example, the domain was included in a link contained in an October 14, 2015 email sent to Azima's email "fa@fa1.us," as shown below.

[51] I observed that, in some cases, the same domains were included in link URLs found in several different emails.



76. According to data published by the Citizen Lab, deferrer[.]website is an indicator of compromise[52] associated with Dark Basin and, by connection, BellTroX and CyberRoot.[53] [54] As part of its investigation of Dark Basin, the Citizen Lab and partner organizations compiled a list of 480 indicators they assess to be associated with Dark Basin and its malicious online activities. The list of indicators includes over a dozen email addresses and hundreds of domains. A sample of the Citizen Lab's data associated with Dark Basin, including the association with the domain deferrer[.]website is shown below.

[52] Threat indicators are data associated with observed forensic data such as URLs, file hashes, or IP addresses that are associated with known cyber threat activity such as phishing, botnets, or malware.

[53] **See:** https://github.com/citizenlab/malware-indicators/blob/master/202006_DarkBasin/iocs.csv

[54] **See:** https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf

master malware-indicators / 202006_DarkBasin / iocs.csv

Preview Code Blame

412	5ede974c-2214-4607-80a7-7a498064ab0b	147	Network activity	domain	budgtoffmy.com
413	5ede974c-2518-4f2b-a1c2-7a498064ab0b	147	Network activity	domain	webmailmanageruk.com
414	5ede974c-2e18-429a-be6d-7a498064ab0b	147	Network activity	domain	com-er-en-us.com
415	5ede974c-40e8-417c-892e-7a498064ab0b	147	Network activity	domain	deferrer.website
416	5ede974c-4364-4cc2-a094-7a498064ab0b	147	Network activity	domain	siteadminhk.com
417	5ede974c-450c-4d31-a992-7a498064ab0b	147	Network activity	domain	zsrvrer.com

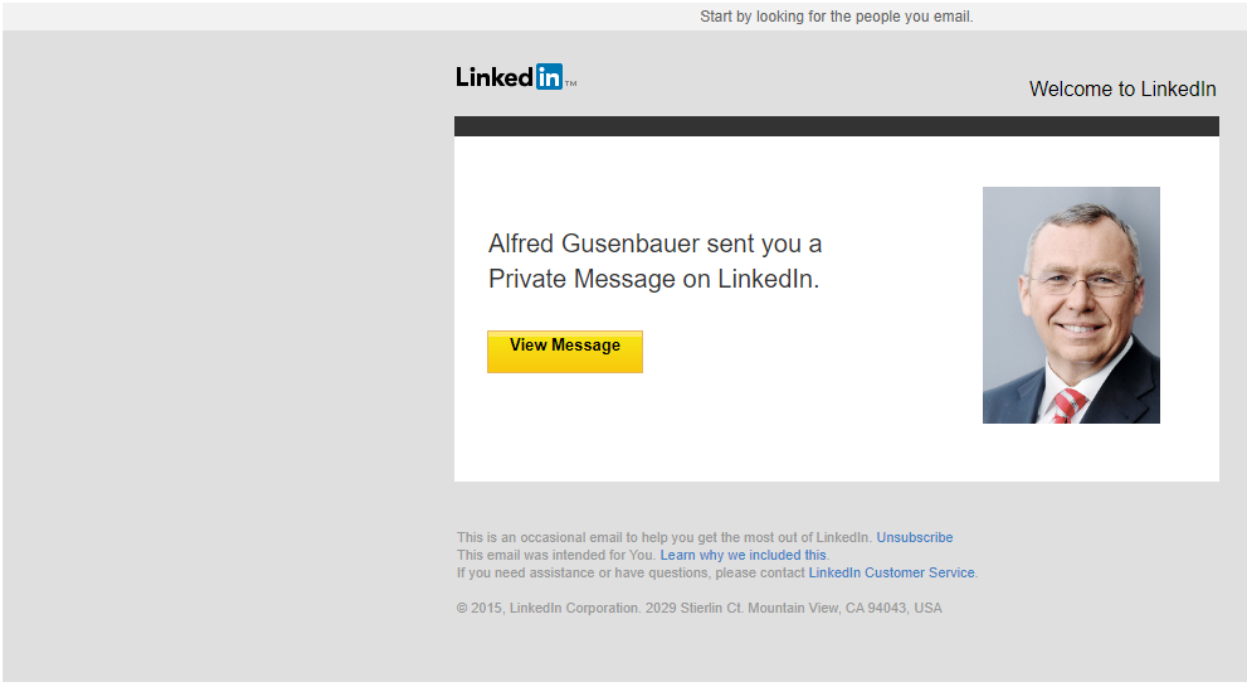
77. I identified an archived screenshot of deferrer[.]website from July 2016 which indicates that the domain appears to have operated as a URL shortening service. URL shorteners allow users to shorten long URLs into a short link. The use of URL shorteners to mask phishing sites or initiate a download of malicious software is a common technique used by hackers.

78. The Citizen Lab investigation of Dark Basin identified 28 URL shortener services operated by Dark Basin, including deferrer[.]website. Screenshots of some of the other URL shortener services operated by Dark Basin included in the Citizen Lab's report closely resemble the archived screenshot of deferrer[.]website. An example of another URL shortener service operated by Dark Basin identified in the Citizen Lab's investigation is shown below left alongside, for comparison, the abovementioned archived screenshot of deferrer[.]website from July 2016, shown below right.

C. look-com[.]org

79. I identified the domain look-com[.]org in a May 19, 2015 phishing email sent to Azima's email address "fa@fa1.us," as shown below.

From: "<Linkedin>" <messages-N0reply-linkedin@tech-center.com>
Sent: 5/19/2015 12:39:47 PM +0200
To: fa@fa1.us
Subject: Alfred Gusenbauer sent you a Private Message on LinkedIn.



Received: (qmail 25709 invoked by uid 30297); 19 May 2015 10:39:54 -0000
Received: from unknown (HELO p3plibsmtp01-12.prod.phx3.secureserver.net) ([72.167.238.228]) (envelope-sender <mes
center.com.cbhebkisudclqyi.mesvr.com>) by p3plsmtp03-05.prod.phx3.secureserver.net (qmail-1.03) with SMTF
Received: from smtp.mesvr.com ([91.103.1.84]) by p3plibsmtp01-12.prod.phx3.secureserver.net with bizsmtp id Vmfs1q00
Received: from smtp.mesvr.com (localhost.localdomain [127.0.0.1]) by smtp.mesvr.com (8.14.4/8.13.8/CWT/DCE) with ES

www.2ntigv4chn2hbk.mesvr.com/tg/2ntigv4chn2hblhttp/accounts-linkedin-com-servicelogin-addsession-v-en-us.look-com.org/-continue-https-maiil.gooogle.com-maiil.u.1.serviice-maiil.r

80. According to data published by the Citizen Lab, look-com[.]org is an indicator of compromise associated with Dark Basin and, by connection, BellTroX and CyberRoot.[55] A sample of the Citizen Lab's data associated with Dark Basin that includes reference to the domain is shown below.

[55] **See:** https://github.com/citizenlab/malware-indicators/blob/master/202006_DarkBasin/iocs.csv

malware-indicators / 202006_DarkBasin / iocs.csv

Preview | Code | Blame | 480 lines (480 loc) · 47.6 KB

418	5ede974c-4ac0-4551-a821-7a498064ab0b	147	Network activity	domain	nigeriaoilleaks.com
419	5ede974c-4f78-44e0-b1d4-7a498064ab0b	147	Network activity	domain	com-biz.website
420	5ede974c-571c-406b-835a-7a498064ab0b	147	Network activity	domain	look-com.org
421	5ede974c-5aa4-4e2b-82b2-7a498064ab0b	147	Network activity	domain	serverforhelpmy.com
422	5ede974c-5f3c-4034-8163-7a498064ab0b	147	Network activity	domain	websitemanagerusa.com

81. By leveraging domain investigations tools to examine the IP addresses historically associated with the domain, I was able to determine that on September 21, 2014, the domain was hosted on IP address 170.178.217.163. On the same date, the same IP address was associated with the domains mail-com[.]org and ppleid[.]org, two domains that the Citizen Lab's investigation revealed to be associated with Dark Basin.[56] A sample of the Citizen Lab's data associated with Dark Basin that lists the two domains is shown below.

malware-indicators / 202006_DarkBasin / iocs.csv

Preview | Code | Blame | 480 lines (480 loc) · 47.6 KB

423	5ede974c-602c-4aa9-bbb0-7a498064ab0b	147	Network activity	domain	ondemand.pushthisurl.com
424	5ede974c-643c-42d9-bae7-7a498064ab0b	147	Network activity	domain	ppleid.org
425	5ede974c-6654-47da-adb0-7a498064ab0b	147	Network activity	domain	mail-msrgr.info
426	5ede974c-6964-4b95-96e4-7a498064ab0b	147	Network activity	domain	com-mail-us.com

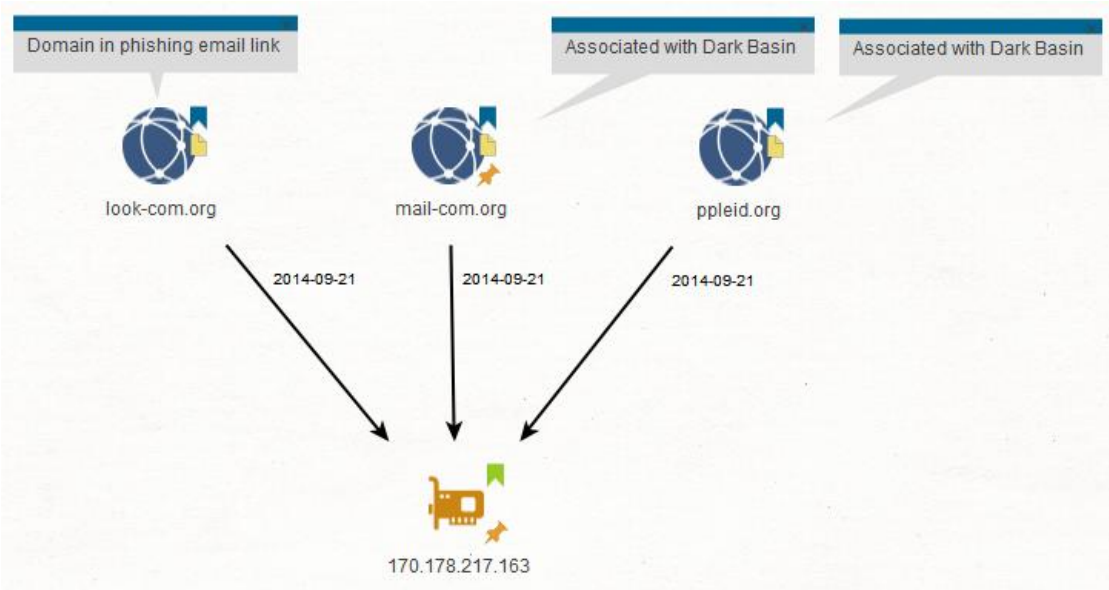
[56] **See:** https://github.com/citizenlab/malware-indicators/blob/master/202006_DarkBasin/iocs.csv

malware-indicators / 202006_DarkBasin / iocs.csv

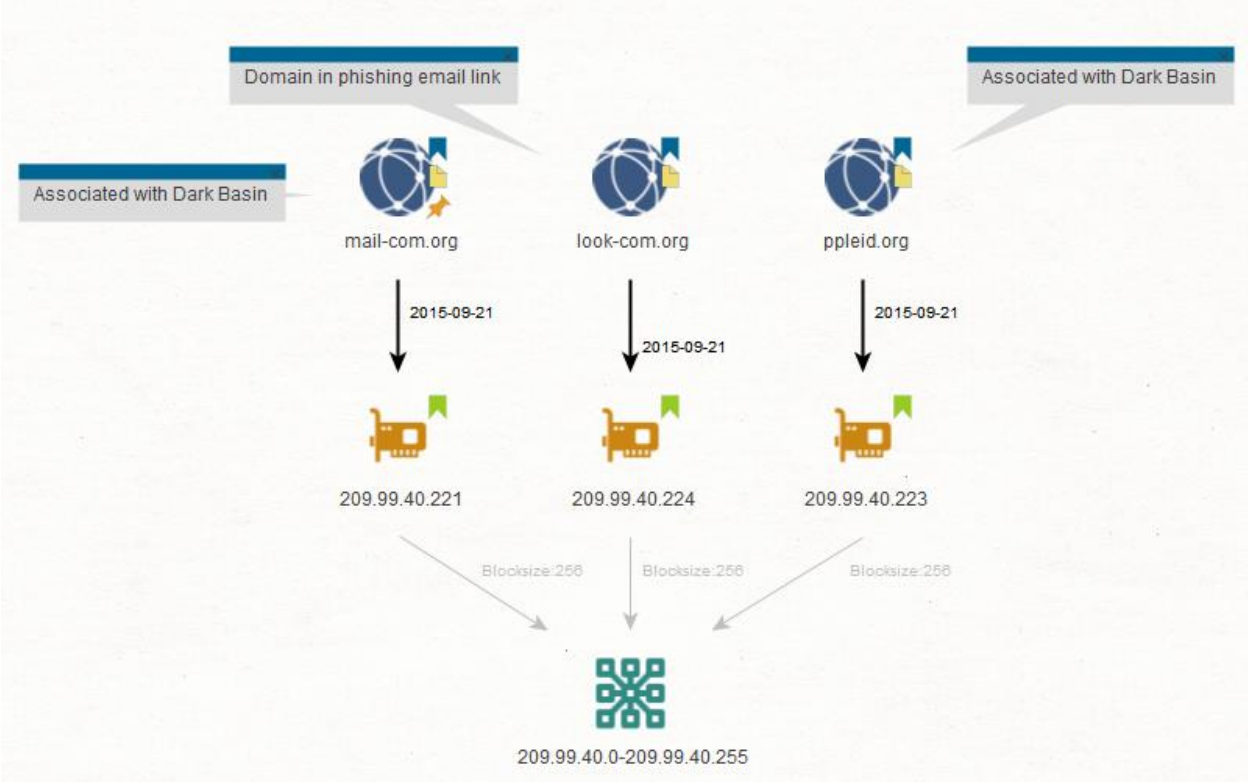
Preview | Code | Blame | 480 lines (480 loc) · 47.6 KB

450	5ede974c-ce54-4e66-a5fd-7a498064ab0b	147	Network activity	domain	msrwr.com
451	5ede974c-d024-4581-b7dc-7a498064ab0b	147	Network activity	domain	mail-com.org
452	5ede974c-d444-40a9-a6e0-7a498064ab0b	147	Network activity	domain	xpertdomain.com
453	5ede974c-d518-4de6-90a3-7a498064ab0b	147	Network activity	domain	com-en-us.co.uk

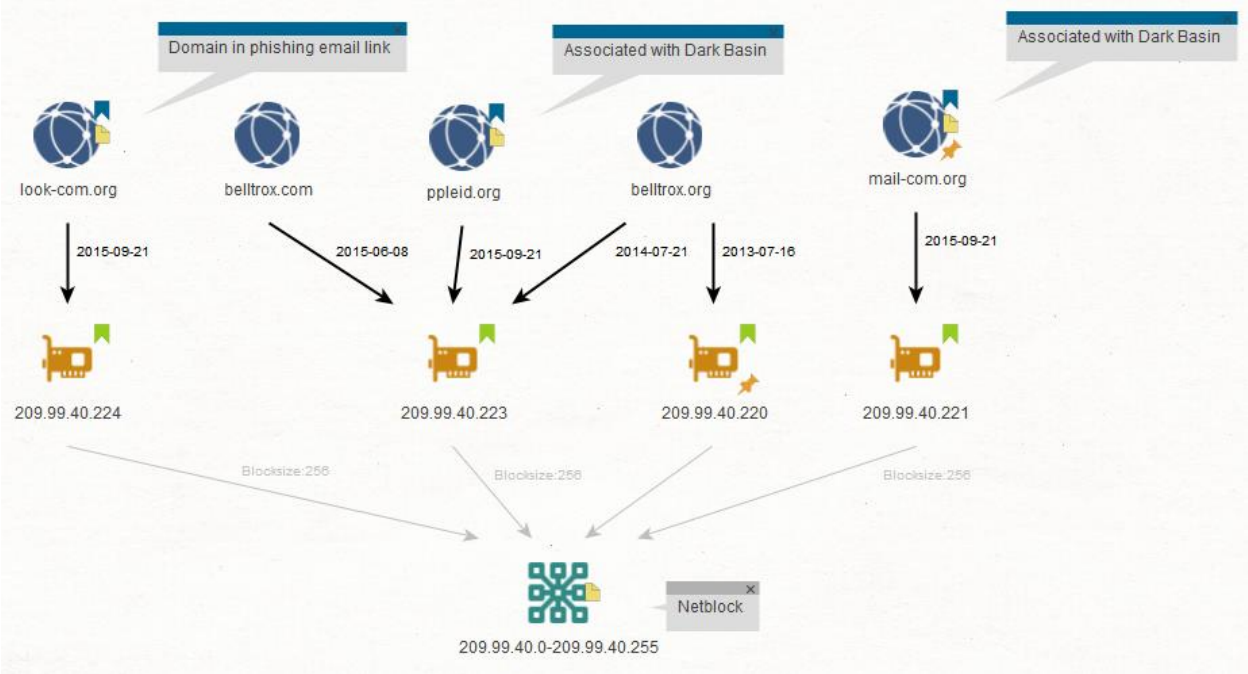
82. Below is a network analysis graphic showing this relationship.



83. On September 21, 2015, approximately four months after the May 19, 2015 phishing email was sent to Azima, look-com[.]org switched to IP address 209.99.40.224. This IP address was part of a netblock—a range of consecutive IP addresses—that mail-com[.]org and ppleid[.]org also switched to on the same date, as shown in the network analysis graphic below.



84. Of additional note, around the same time, the same netblock was tied to two domains associated with BellTroX: belltrox[.]org and belltrox[.]com. The domain belltrox[.]org was associated with IP address 209.99.40.223 (the same IP address associated with ppleid[.]org) on July 21, 2014, and IP address 209.99.40.220 on July 16, 2013. On June 8, 2015, belltrox[.]com was also associated with IP address 209.99.40.223. All the IP addresses are part of the same netblock, as shown in the network analysis graphic below.



85. I further note that the five domains were all registered by the same registrar, "PDR Ltd. d/b/a PublicDomainRegistry.com (R27-LROR)" ("PDR"), during approximately the same time period.

Domain	**Dates Associated with PDR** (as indicated in domain registration records)
look-com[.]org	9/21/2014 - 12/4/2015 (Sponsoring Registrar)
mail-com[.]org	9/21/2014 - 12/4/2015 (Sponsoring Registrar)
ppleid[.]org	9/21/2014 - 12/4/2015 (Sponsoring Registrar)
belltrox[.]com	9/3/2012 – 6/9/2018 (Registrar)
belltrox[.]org	7/27/2013 – 9/28/2014 (Sponsoring Registrar)

86. I identified a domain registration record associated with look-com[.]org from September 21, 2014 that contains the registrant email "plakesr@gmail.com" along with various other registrant information. I conducted searches and identified the same email listed as the registrant in domain registration records associated with mail-com[.]org and ppleid[.]org on September 21, 2014, as well as several other domains. I conducted searches for the

"plakesr@gmail.com" email address in our proprietary breached records database[57] and identified seven records, several of which indicate the email is associated with an individual named "Arun Sharma" ("Sharma") with a reported location of Jaipur, India. I also conducted searches across hundreds of social media accounts and discovered a Google account under the name "Arun Sharma" directly connected with the email, providing further corroborating information to indicate the email is connected with an individual with that name. We also identified at least five social media accounts associated with Sharma under the same username as the email handle, "plakesr."

87. Among registration records for other domains, Sharma's identifying information and the email "plakesr@gmail.com" were identified in domain registration records from between March 2013 and June 2013 for the domain 82servers[.]com. I identified approximately half-a-dozen archived captures of webpages from the domain from this time period which indicate it served as the website for IT services and webhosting company 82Servers based in Jaipur, India. We also identified Sharma's identifying information in domain registration records from between April 2012 and June 2014 for 82servers[.]in. I identified a LinkedIn account for Sharma that reports employment as a "System Admin" at 82Servers.[58]

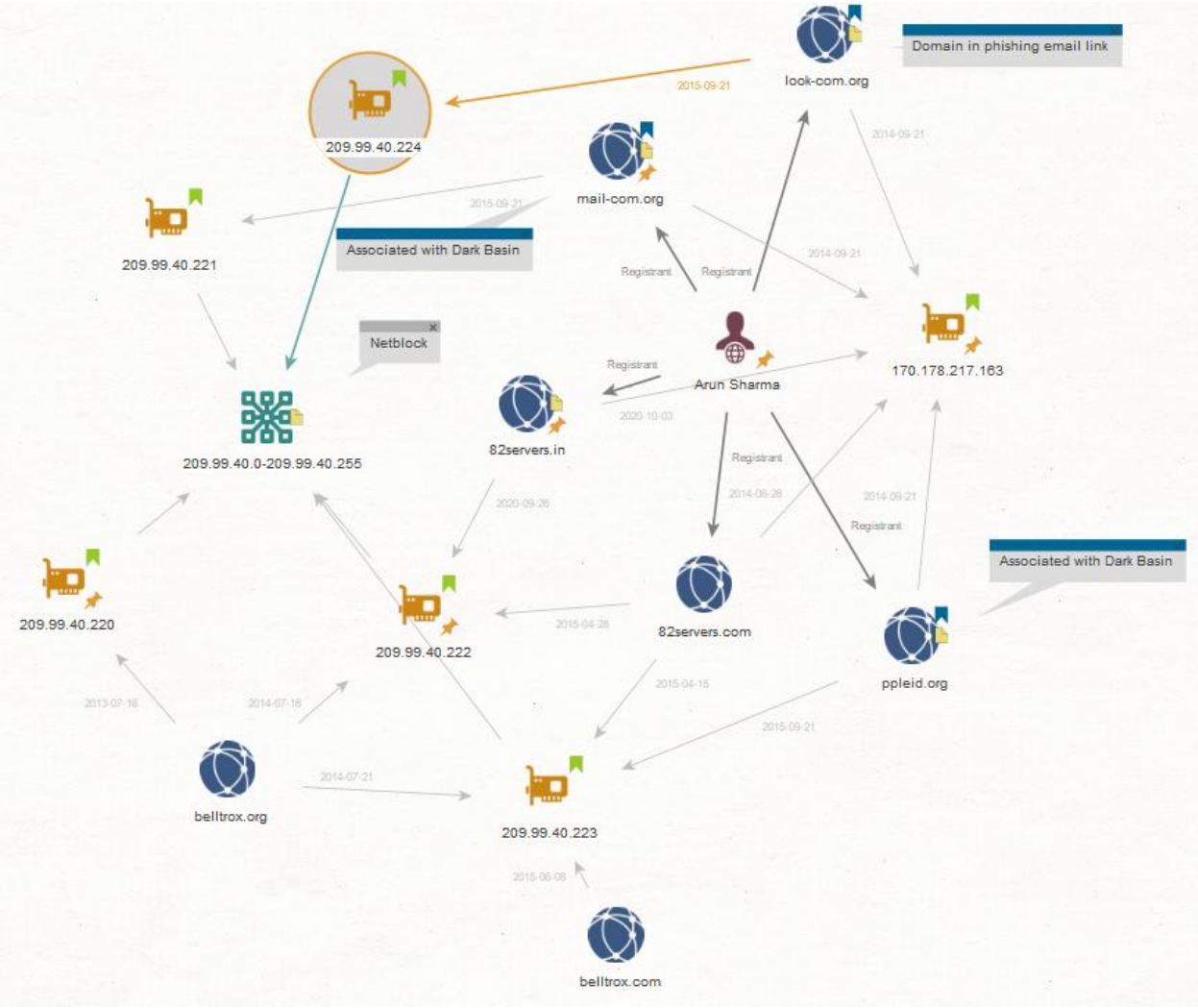
88. In October 2020, 82servers[.]in was associated with the IP address 170.178.217.163. The same IP address was connected with look-com[.]org, mail-com[.]org, and ppleid[.]org in 2014. In April 2015 and September 2020 82servers[.]com and 82servers[.]in, respectively, were associated with the IP address 209.99.40.222, which is part of the same netblock connected with look-com[.]org, mail-com[.]org, ppleid[.]org, belltrox[.]com, and belltrox[.]org. Given that Sharma's email was identified in domain registration records for the CyberRoot /

[57] Our proprietary database is a repository with tens of billions of compromised records and other person of interest data collected from the Deep and Dark Web over the past decade.

[58] **See:** https://www.linkedin[.]com/in/arun-sharma-10814357/

BellTroX associated domains look-com[.]org, mail-com[.]org, and ppleid[.]org, and that he is also associated with 82servers[.]in, which shares the same network infrastructure as these domains, they appear to be linked.

89. A network analysis graphic showing these connections is included below.



D. Conclusion

90. It is my opinion that it is likely that the shared characteristics described above are an indication that the domains were operated and/or created by the same individual(s) or organization(s). Furthermore, given the characteristics of the domains and IP addresses detailed

above as well as the forensic data discovered by the Citizen Lab, it is my opinion that the domains are associated with CyberRoot. Accordingly, it is my opinion that at least seven of the phishing emails sent to Azima and his associates were likely associated with CyberRoot.

Respectfully submitted,

Matteo Tomasini

Matteo Tomasini

DISCLOSURE

The information contained herein does not constitute a guarantee or warranty by Prescient Comply LLC, its subsidiaries, branches and/or affiliates ("Prescient") of future performance nor an assurance against risk. Prescient's work and findings shall not in any way constitute recommendations or advice regarding the client's ultimate commercial decision, which shall, in all respects, remain the client's own. This report is for the benefit of the client only (including its directors, officers, and employees) and may not be disclosed to any third parties without the prior written consent of Prescient. Copyright © Prescient. All rights reserved. This document cannot be reproduced without the express written permission of Prescient. Any reproduction without authorization shall be considered an infringement of Prescient's copyright.

July 3, 2024

SUPPLEMENT TO EXPERT REPORT OF MATTEO TOMASINI

Farhad Azima v. Nicholas Del Rosso & Vital Management Services, Inc, United States District Court for the Middle District of North Carolina, 20-cv-954 (Internal Ref. No. 47776373)

I. BACKGROUND ON SUPPLEMENTAL REPORT

1. I submitted my initial expert report on May 24, 2024. Miller & Chevalier Chartered ("Miller" or the "Firm") subsequently provided me with a June 24, 2024 rebuttal report authored by Defendants' expert witness, Lee Whitfield ("Whitfield" or "Mr. Whitfield"). Nothing in the rebuttal report alters the conclusions I reached in my expert report. However, in the interest of providing further supporting information regarding the conclusions asserted in my previous report, I wish to submit the following supplement.

II. SUPPLEMENTARY SUPPORTING INFORMATION

A. Credibility Of the Citizen Lab Investigation of Dark Basin / BellTroX

2. As described in my expert report, my investigation of the identifiers associated with the phishing emails sent to Mr. Azima and his associates led me to review and analyze a report and data published by the Citizen Lab[1] titled "Dark Basin: Uncovering a Massive Hack-For-Hire Operation" that focuses on Dark Basin, a hack-for-hire group that the Citizen Lab links to BellTroX with "high confidence."[2]

3. Based on my expertise as a cyber security expert, the Citizen Lab is a credible organization and well-respected source for cyber threat intelligence research within the cyber security sector. The Citizen Lab conducted over two years of research as part of its investigation. Its methodology appears to have been rigorous, including the collection and analysis of an extensive amount of threat actor data in order to build a detailed picture of the phishing operations and campaigns operated by BellTroX / Dark Basin. As such, I have no reason to doubt the validity of the Indicators of Compromise they identified as being associated with BellTroX / Dark Basin

[1] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada, that conducts research on information and communication technologies, human rights, and global security. It is considered a credible source when it comes to spyware research.
[2] **See:** https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf

which I considered as part of my investigation of the phishing emails.

4. Another reason why I find the Citizen Lab's conclusions credible is that the organization collaborated with NortonLifeLock, who conducted a parallel investigation[3] into Dark Basin,[4] and who jointly released the list of Indicators of Compromise associated with BellTroX / Dark Basin that I utilized as part of my investigation of the phishing emails. NortonLifeLock, now known as Gen Digital Inc., is a leading multinational cybersecurity software and services company whose cyber threat intelligence research is also well respected in the cyber security sector, providing further credibility to the data I utilized to form my conclusions. As a testament to the credibility of the organizations and their work, technical information from their investigation has reportedly been shared with the U.S. Department of Justice and law enforcement agencies in multiple countries.

B. Connection Between BellTroX and CyberRoot

6. As explained in my initial report, my basis for connecting BellTroX to CyberRoot is a December 2022 report authored by Meta titled "Threat Report on the Surveillance-for-Hire Industry" ("Meta Report"). The Meta Report analyzes CyberRoot and alleges it is a surveillance-for-hire firm, i.e., a hacking firm.[5] It also concludes that CyberRoot uses tactics similar to those of BellTroX and that, according to public reporting, CyberRoot and BellTroX have a history of working together and have shared the same web infrastructure and employees.[6] [7] The Meta Report is an independent third-party report that uses reliable methodology and sources.

[3] **See:** https://web.archive.org/web/20200826081745/www.nortonlifelock.com/blogs/security-response/mercenary-amanda-professional-hackers-hire
[4] Referred to by NortonLifeLock as "Mercenary.Amanda."
[5] **See:** https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf
[6] **See:** https://www.reuters.com/article/cyber-lawsuit-belltrox/lawsuit-accuses-indian-hackers-of-leaking-businessmans-emails-idUSKBN2742EN/
[7] **See:** https://www.bloomberg.com/news/articles/2020-10-19/u-s-businessman-says-hacker-for-hire-firms-stole-his-data

DISCLOSURE

The information contained herein does not constitute a guarantee or warranty by Prescient Comply LLC, its subsidiaries, branches and/or affiliates ("Prescient") of future performance nor an assurance against risk. Prescient's work and findings shall not in any way constitute recommendations or advice regarding the client's ultimate commercial decision, which shall, in all respects, remain the client's own. This report is for the benefit of the client only (including its directors, officers, and employees) and may not be disclosed to any third parties without the prior written consent of Prescient. Copyright © Prescient. All rights reserved. This document cannot be reproduced without the express written permission of Prescient. Any reproduction without authorization shall be considered an infringement of Prescient's copyright.